2

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

SECURITY CONSIDERATIONS
IN DISTRIBUTED SYSTEMS

by

Donovan Ross Rhead

September 1991

Thesis Co-Advisor: Myung Suh
Thesis Co-Advisor: Moshe Zviran

Approved for public release; distribution is unlimited

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION Unclassified		1b RESTRICTIVE MARKINGS	
2a SECURITY CLASSIFICATION AUTHORITY		3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.	
2b DECLASSIFICATION/DOWNGRADING SCHEDULE			
4 PERFORMING ORGANIZATION REPORT NUMBER(S)		5 MONITORING ORGANIZATION REPORT NUMBER(S)	
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b OFFICE SYMBOL *(If applicable)* 37	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School	
6c ADDRESS *(City, State, and ZIP Code)* Monterey, CA 93943-5000		7b ADDRESS *(City, State, and ZIP Code)* Monterey, CA 93943-5000	
8a NAME OF FUNDING/SPONSORING ORGANIZATION	8b OFFICE SYMBOL *(If applicable)*	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c ADDRESS *(City, State, and ZIP Code)*		10 SOURCE OF FUNDING NUMBERS	

Program Element No	Project No	Task No	Work Unit Accession Number

11 TITLE *(Include Security Classification)*
Security Considerations in Distributed Systems

12 PERSONAL AUTHOR(S) Rhead, Donovan R.

13a TYPE OF REPORT Master's Thesis	13b TIME COVERED From To	14 DATE OF REPORT *(year, month, day)* September 1991	15 PAGE COUNT 102

16 SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 COSATI CODES

FIELD	GROUP	SUBGROUP

18 SUBJECT TERMS *(continue on reverse if necessary and identify by block number)*
Distributed System; Network; Security; Countermeasure; Control

19 ABSTRACT *(continue on reverse if necessary and identify by block number)*

This thesis investigates computer security considerations in distributed systems. In particular, it concentrates on assisting managers to gain an appreciation for what distributed systems are, and what are the inherent security issues in these systems. A survey of the literature on computer security was conducted to identify those issues unique to distributed systems. Although many controls are discussed, management must design and support a comprehensive security plan tailored to their unique organization.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS REPORT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a NAME OF RESPONSIBLE INDIVIDUAL Moshe Zviran	22b TELEPHONE *(Include Area code)* (408) 646-2489	22c OFFICE SYMBOL AS/Zv

83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

Security Considerations
in
Distributed Systems

by

Donovan R. Rhead
Lieutenant, United States Navy
B.S., Wayne State University, 1983

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
September 1991

Author: ______________________________
Donovan R. Rhead

Approved by: ______________________________
Myung Suh, Thesis Co-Advisor

____
Moshe Zviran, Thesis Co-Advisor

______________________________ for
David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

This thesis investigates computer security considerations in distributed systems. In particular, it concentrates on assisting managers to gain an appreciation for what distributed systems are, and what are the inherent security issues in these systems. A survey of the literature on computer security was conducted to identify those issues unique to distributed systems. Although many controls are discussed, management must design and support a comprehensive security plan tailored to their unique organization.

TABLE OF CONTENTS

I. INTRODUCTION

Security threats and countermeasures are well identified for stand-alone computer system assets. Rapid technology advances, however, have changed the form and extent of connectivity between computer systems and enhanced the use of distributed architectures (Buchanan and Linowes, 1980). Distributed computer systems face the same potential threats as stand-alone systems plus additional threats stemming from their unique characteristics. Reasons for the increased security exposure may include: (Johnson and Layne, 1987; Muftic, 1989)

- Geographic dispersion of computer system assets
- Several organizations and management involved in a single network
- Central control is difficult
- Dissimilar computers and operating systems
- More entities involved
- Security exposure over a broader range of levels

A comprehensive examination of threats to such systems, including those threats stemming from system connectivity is essential to any security plan. (Pfleeger, 1989)

The main objective of any security plan is to operate systems at an acceptable level of risk. The scope of a security program should be commensurate with the value of the assets requiring protection. Typical grouping of these assets are hardware, software, data, personnel, documentation and supplies. A more extensive list of possible assets is provided in Appendix A and will be further discussed in Chapter III.

Distributed system security employs management implemented countermeasures to ensure the protection of assets in a distributed environment. It provides assurances that the distributed system performs critical functions correctly. While security goals for stand-alone systems are well known, the goals unique to distributed systems are more complex and difficult to identify (IBM, 1987; Branstad, 1987). These goals include system integrity, connection confidentiality, originator/recipient nonrepudiation, access control, and denial of service. (COMNAVDAC, 1991; Stallings, 1990)

System Integrity. System integrity provides for the integrity of all user data on all connections. It can be further broken down into three subcategories. The first involves the routing of data where data transmitted from any point in a network is received at the intended destination and nowhere else. The second involves the protection of data itself where the data received at any point in a distributed system is exactly the same in content as the data transmitted. It allows for the determination of whether the data has been modified, inserted, deleted, or replayed. Thirdly, it guarantees that information, while in transit, cannot be observed, tampered with, or extracted from the distributed system by some unauthorized person or device.

Connection Confidentiality. Provides for the confidentiality of all user data on a connection.

Originator/Recipient Nonrepudiation. Another goal of distributed system security is to assure *nonrepudiation*. It provides the sender of data with proof of data delivery to protect against any attempt by the recipient to deny receiving the data. It also provides the data recipient with proof of data origin to protect against any attempt by the sender to deny sending the data. It must also allow for the sender of the data to verify that receipt was by (and only by) the authorized recipient.

Access Control. Access control guards against unauthorized access to a resource such as reading, writing, or deleting data. It guarantees that all physical components of the distributed system on the organization's premise are accessible only to authorized individuals. Examples of physical components include terminals, terminal controllers, modems, nodes, data links, and telecommunication lines. Access control also detects and identifies any attempt to observe, tamper with, or extract information from the network by an unauthorized person or device. Once a known violation has occurred an appropriate action can be taken to prevent future occurrences.

Denial of Service Protection. Adequate alternate paths allow transmission of data between points in a distributed system where the need for transmission of data exists. These paths also ensure that alternate means of transmitting has been identified, implemented, and tested. For critical data, contingencies should address failure by the primary and backup paths.

This thesis focuses on security threats unique to distributed systems. The investigation begins by identifying characteristics and assets of distributed systems. Security threats unique to distributed systems are then identified, with an analysis of possible countermeasures for the identified threats.

II. DISTRIBUTED SYSTEM OVERVIEW

A. DEFINITION

There is not a universally accepted definition to the term *distributed systems.* Rather, it describes information systems with widely different architectures and characteristics. The absence of such a definition suggests that it is as much a point of view as a system type with distinguishing characteristics. There are two fundamental attributes that all distributed processing systems seem to have in common: (Lorin, 1988)

1. There are multiple instances of stand-alone computer systems.
2. The stand-alone systems can communicate electronically.

When attempting to evaluate a system, a diagram can show how pieces of equipment are connected. Diagrams of the system structure, or topology, can be helpful but do not fully describe the system. Four other important characteristics should also be included. (McNurlin and Sprague, 1989)

1. Where the processing is performed
2. What communication links are used
3. Where the information is stored
4. What rules or standards are in place

B. MODES OF DISTRIBUTED PROCESSING

Rapid technological advances continue to impact interconnect capability, processor capacity, software methodology, and industry pricing structures. These changes have expanded the set of designs available in solving information processing problems (Ahituv and Sadan, 1985). The significance of the distributed processing lies in the variety of systems choices allowing organizations to better fit the information system architecture to their own organizatic .al structure (Buchanan and Linowes, 1980). Figure 1 displays the continuum of systems that exist between stand-alone and highly distributed systems.

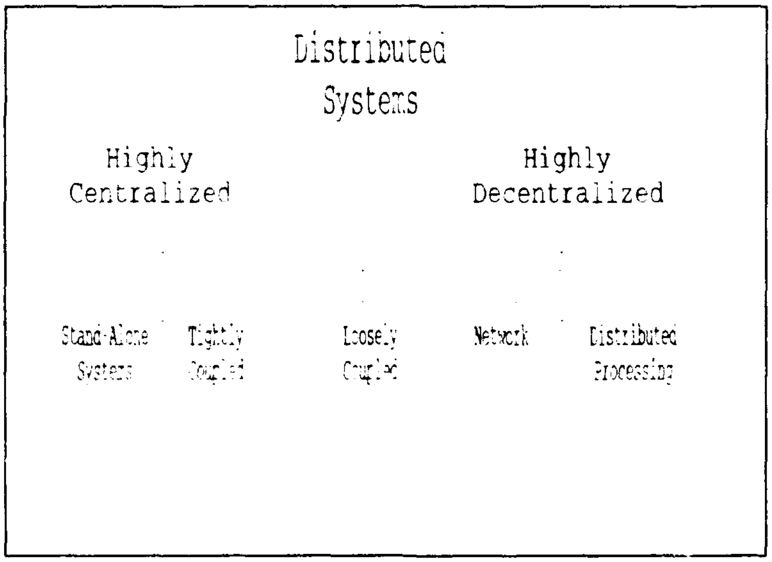

Figure 1 Distributed System Continuum

The following grouping of systems based on the degrees of the two fundamental attributes of multiple nodes and electronic communication are identified for comparison.

Stand-alone Systems. A stand-alone system is one that can be treated as a distinct entity. There is no form of electronic communications to any other system.

Tightly Coupled Systems. Tightly coupled systems are multiprocessor systems. They are a population of processors sharing addressing to memory and devices. This sharing is accomplished by utilizing single operating system. The existence of a single operating system results in the presence of a space-time coherence between the processors. A unit where space-time coherence exists can be managed as a single node. A node is an element of a computer network.

Loosely Coupled Systems. The loose interconnection of computer systems comes very close to the concept of distributed processing by the attribute of multiple complete systems. They are systems connected over I/O pathways, traditionally distinct from networks. Many of these pathways differ from tightly coupled systems only in the physical sense that they do not share memory or operating systems. They may be functionally quite dependent, and as a result take on the characteristics of a single node, a single 'system', rather than an interconnection of two nodes.

Networked Systems. There are many types of networks displaying a broad range of characteristics. They can vary from completely autonomous systems with the added ability to communicate electronically, to diskless workstations completely dependent on the network server for all secondary storage and communications operations. Each type of network has some unique set of properties that makes it attractive based on service provided, cost, reliability, serviceability, flexibility, etc. As well, each unique network possesses some set of properties that make it similar in nature to other network types.

C. NETWORKED SYSTEM

A second approach at identifying and grouping distributed systems can be accomplished through the examination of system structures. By this approach four system structures that qualify as distributed are identified. (McNurlin and Sprague, 1989)

A hierarchy of processors. This structure is typically the most common in larger information systems that have shifted toward increased distribution and end-user computing. Topographically, the largest computer resides at the top and personal computers or terminals at the bottom, as displayed in Figure 2. At least three possible schemes for data storage can be supported by this particular organization. First, all data can be stored at the top of the hierarchy. Secondly, master records can be stored at the top, with subsets at intermediate levels to support lower level processing. Thirdly, master records can be stored where they are most used and provide updated records to the top of the hierarchy for backup purposes.

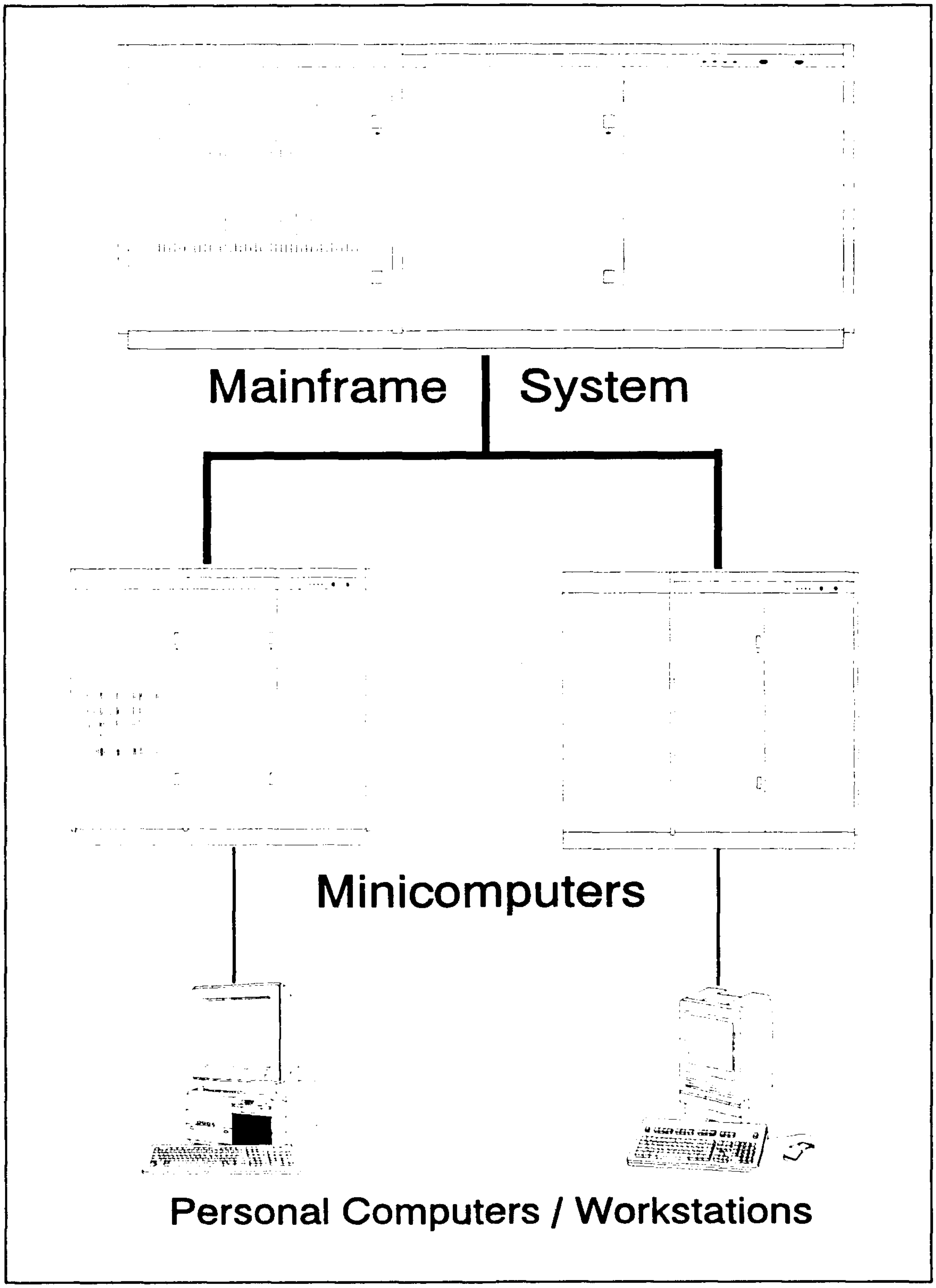

Figure 2 Hierarchy of processors.

A network of cooperating workstations. This structure is common for current office systems. An example is displayed in Figure 3.

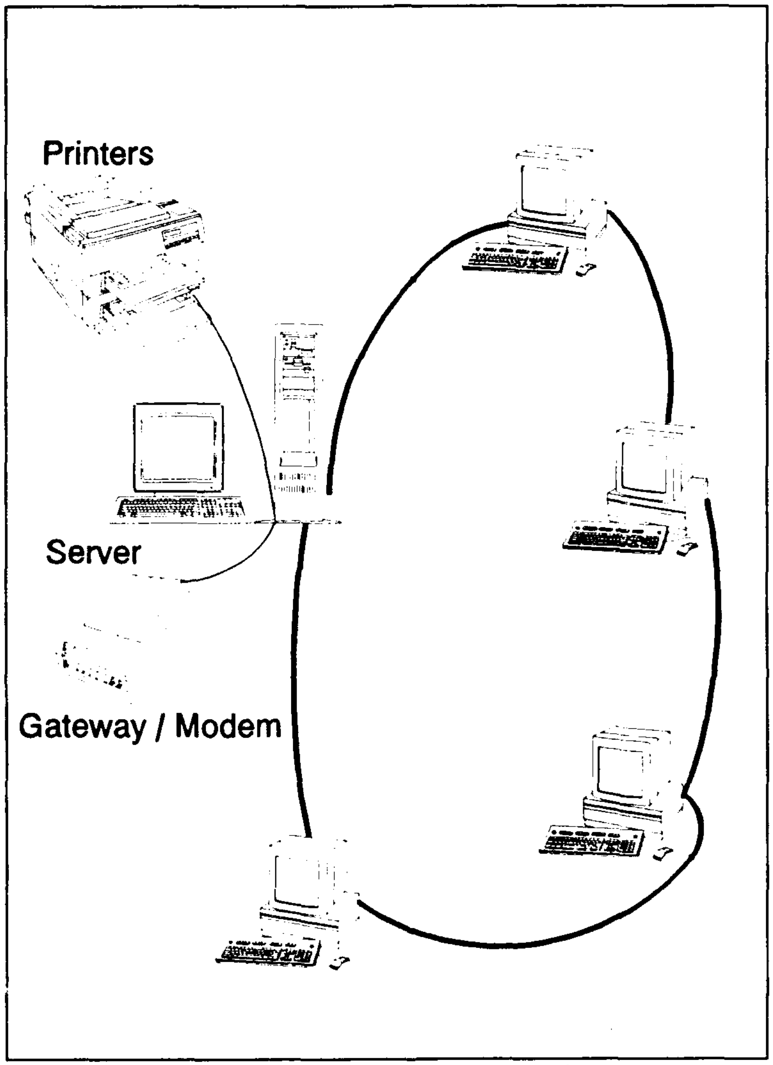

Figure 3 Cooperating workstations.

There is no particular hierarchy of processors. Any workstation can call on another workstation in the network for data or service, provided it is authorized to do so.

Decentralized stand-alone systems. Decentralization is the dedication of applications to systems in such a way that systems do not interact with each other as shown in Figure 4.

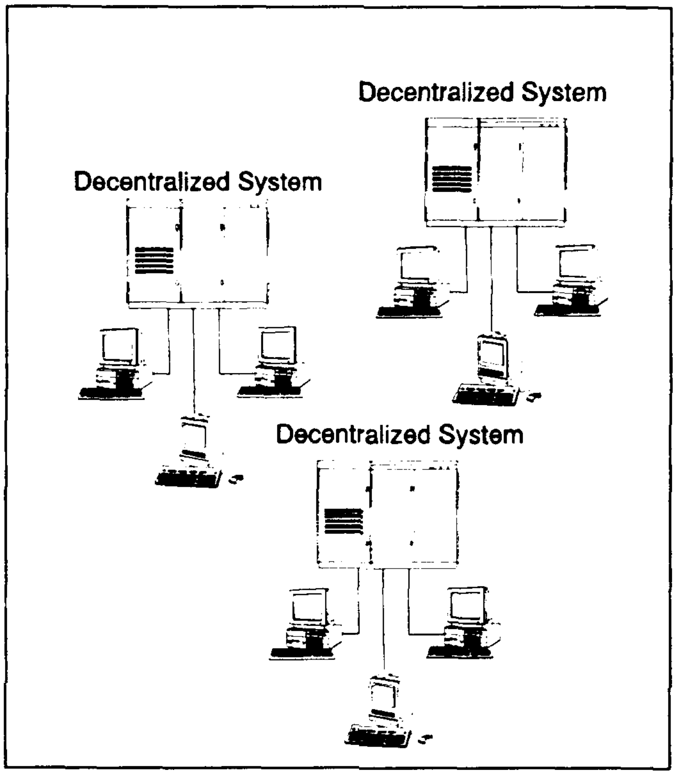

Figure 4 Decentralized stand-alone systems.

It occurs when applications that have traditionally been sharing a large machine are moved to several smaller systems. This is frequently seen in organizational information systems originally designed in the 1960's where many small data centers existed within a large organization. These independent systems have been subsequently modernized to allow a little data to flow among the decentralized systems, but mostly in an upward direction toward corporate management.

Office systems that communicate with data processing. This structure is a hybrid of two other identified structures. As displayed in Figure 5, it is a combination of the hierarchy approach (for Data Processing) and the network of cooperating workstations (for office systems).

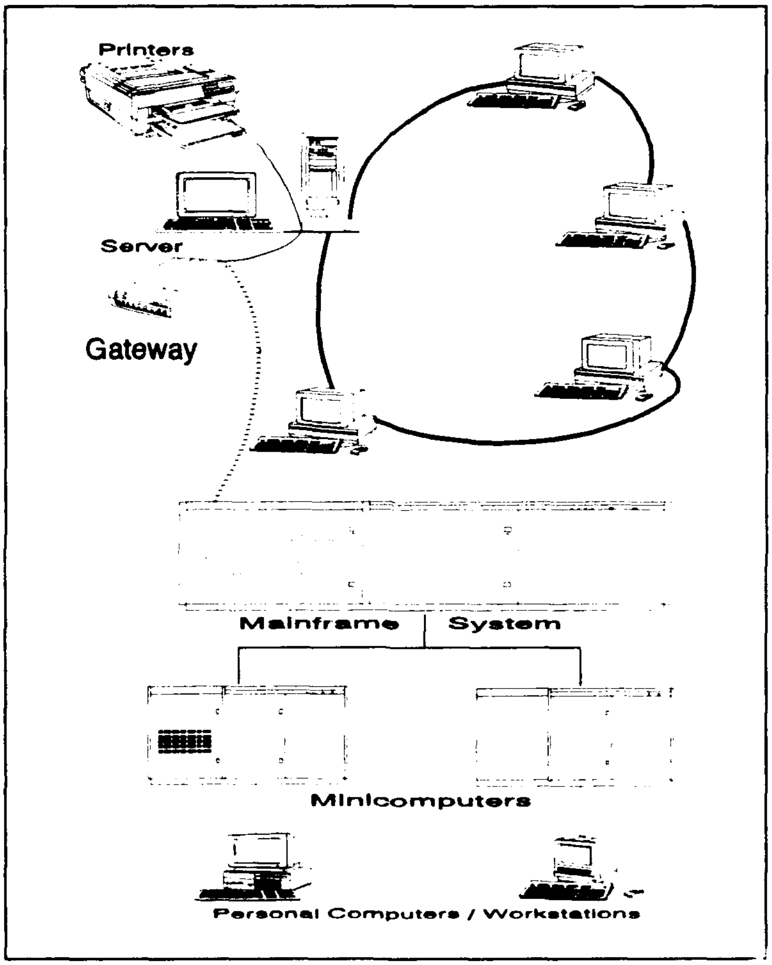

Figure 5 Office systems that communicate with data processing

Each of these four network architectures discussed previously need additional specification to describe fully the degree to which it is distributed. These additional factors are:

Distributed processing. An important distinction must be ma1e between decentralized and distributed processing. Distributed processing contains some concept of system, of node relations, dependency, and interaction. It provides for the processing of an application on a computer that is located outside the corporate data center and operates on a network. In its ideal form it is a mapping of a single application across several nodes. The goal is to move processing closer to the user or to use different machines to do the part of a job each does best. A distributed system is a system in the sense that there is interaction, cooperation, and some form of dependency between nodes.

One current form of distributed processing is based on the concept of cooperative processing. These systems operate by dividing processing between two or more geographically dispersed nodes. After completion of processing, one node sends data to another node for further processing.

All forms of distributed processing are dependent on the cooperative effort of the system's nodes. More advanced forms of distributed processing are possible with increased interoperability. Interoperability is the capacity for nodes using different operating systems and different hardware platforms protocols to work together on the same task. Node interoperability can be supported in two forms:

- Transparent communication between system applications using system protocols.

- The interactive or two-way flow of messages between user applications.

Connectivity among processors. Each processor in a distributed system can send data and messages to any other processor through electronic communication linkages. A clear trait of electronic communication is that as distance grows, the communication gets slower, less reliable, and more expensive. Breakpoints based on distance have been accepted because of orders of magnitude differences in speed and reliability. These are often grouped as : In-Frame, Bus, Local-Area, Metropolitan-Area, and Wide-Area, and Global Interconnection. Emerging communications technology is beginning to provide interconnect pathways at speeds sufficient to blur the importance of physical distance. The reliability of node interconnection is also dependent on the availability of alternate communication paths.

Distributed databases. As seen in the discussion of systems displaying a hierarchy of processors, the location of data storage is an important design consideration. Two possible avenues are available based on the duplication of data. The first is dividing a database and distributing its portions throughout a system without duplicating the data. Any portion of the data should be accessible from any node, subject to access authorizations. Data location is transparent to users, it is the system's responsibility to know where all data is stored. The second possible avenue is based on distributed duplicate data. In this approach the same data is stored at several locations, although one site generally contains the master file. Here, the system is responsible for synchronizing data which can be a significant problem.

System-wide rules. The shift away from centralized systems and toward distributed systems is making connectivity more important than in the past. This shift permits greater control of operations by components of an organization, yet can potentially degrade connectivity. Operating discipline for the entire distributed system needs to be developed and enforced at all times. These rules include intercommunication between nodes, security, data accessibility, program and file transfer, and common operating procedures.

III. DISTRIBUTED SYSTEM ASSETS AND THREATS

There is an interrelationship between assets and potential threats (see Figure 6).

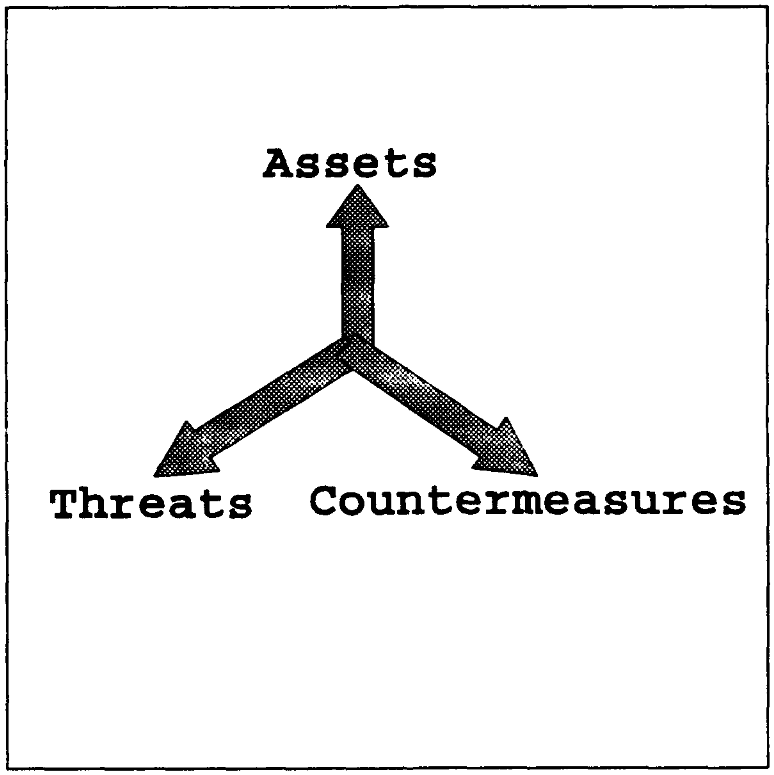

Figure 6 Relationship Between Assets, Threats, and Countermeasures.

Security plans are a tailored application of countermeasures to protect assets against threats.

A. ASSETS

An asset is any resource of value to an organization. Some assets are easily defined or tangible. Other assets are more difficult to identify. Types of information system assets are grouped as hardware, software, data, facilities, personnel, documentation and supplies (Pfleeger, 1989). Examples of assets within each of the identified categories are:

- Hardware: Storage devices such as disk and tape drives.
- Software: System utilities.
- Data: Confidential or proprietary information.
- Facilities: Environmental systems such as air conditioning.
- Personnel: Systems analysts or consultants.
- Documentation: Of security policy test and evaluation.
- Supplies: Paper and printer ribbons.

For a more complete list of potential system assets, see Appendix A (COMNAVDAC, 1991). The degree with which a system is distributed changes the scope and value of these assets.

B. THREATS

A *threat* is a circumstance that has the potential to cause loss or harm. (Pfleeger, 1989) Threats exhibit varying degrees of detectability and controllability. Fire is an example of a threat which is easily detectable and controllable. Natural disasters such as floods are easily detected but difficult to control. Wiretapping lines of communication or infection by computer virus are examples of threats which are neither easily detected nor controlled.

As in a stand-alone system, threats in a distributed environment may impact assets in four ways: (COMVAVDAC, 1991)

- Modification: Altering an asset by changing its representation or adding more to the representation.
- Destruction: The asset is not reparable or recoverable.
- Disclosure: Information is accessed by or released to someone lacking a need-to-know.
- Denial of services: Resources are unavailable to authorized users.

Distributed systems have complicated computer security. As computer systems are moved from their well protected centralized facilities to unprotected offices, there is an increase in the vulnerability of these systems. Among the features of distributed systems that lead to vulnerabilities are: (McNurlin and Sprague, 1989; Johnson and Layne, 1987)

- The distribution of hardware
- The distribution of software
- The distribution of data
- The distribution of computer expertise
- The distribution of documentation
- The distribution of output
- Different security policies

- Different interfaces
- Incompatible security architectures
- Composite risks
- Lack of strong technical history in network security
- External exposure of communications media and facilities

Distributed systems move the actual processing capability to end users. End users gain physical and logical control of many assets once under the control of the computer or information systems department. This shift in control often entails a shift in responsibility for protection of the system's assets. (Ahituv and Sadan, 1985) The same assets present in centralized systems are present in distributed systems. It is the change in the environment that leads to changes in threats to the system. (McNurlin and Sprague, 1989)

Some assets are easily valued by purchase or development costs. The valuation of other assets, such as information, is organizationally dependent. (Clark and Wilson, 1987) An examination of distinct approaches by the Department of Defense (DOD) and major corporations can highlight this dependency. (Chalmers, 1986)

The DoD has prioritized potential impacts of threats and has placed disclosure of information as its top concern. (Winters, 1990) It also has a long standing and highly formalized methodology for the classification and protection of information. Management has determined the value of the information. The classification of information processed and the type of accesś allowed dictates what pre-defined minimum security requirements must be met by any system. System managers must use available technology to meet these difficult goals (if possible) without regard to cost or impact cf the countermeasures on the organization. (Johnson and Layne, 1987)

The corporate approach has prioritized potential impacts by threats on its assets and has placed modification (integrity) of information as its top concern. (Winters, 1990) Corporations tend to treat information as an asset with an identifiable financial value. It is a management decision to value information and to decide what countermeasures are cost efficient. Management must also consider the countermeasure's impact on organizational operations. (IBM, 1987)

C. SOURCES OF THREATS

The environment in which information exists influences how threats may impact assets. A historical review of sources of exposure to financial loss can be useful in constructing a security plan. These exposures can vary significantly depending upon the nature of the establishment and the degree of management controls in place. One example of such reviews was conducted by IBM. This study shows that personnel within the organization may be the greatest source of threats. (IBM, 1987) A similar study recently conducted further demonstrates that personnel with approved access represented the greatest threat to information systems. (Jackson, 1990) A summary of the report is shown below:

- Insider threats: 70% to 80% of Annual Dollar Loss
- Physical threats: 20% to 25% of Annual Dollar Loss
- Outsider threats: 1% to 3% of Annual Dollar Loss

The shift toward end-user computing and distributed systems make security by physical isolation impracticable.

D. ATTACKS ON INFORMATION IN TRANSIT

Attacks against information may occur while in transit or in storage (see Figure 7). Controls designed to protect information in storage are well understood. The same countermeasures applicable to stand alone systems are also applicable to distributed systems.

Information in transit is inherently insecure because the telecommunication process itself is insecure. Both information in transit and the telecommunication process are insecure for two reasons. First, the telecommunication service provider has been isolated from any legal obligation to protect the confidentiality of the information that moves through its facilities. Secondly, securing data communications would require both investment and technical innovation by telecommunication service providers. (Menkus, 1990)

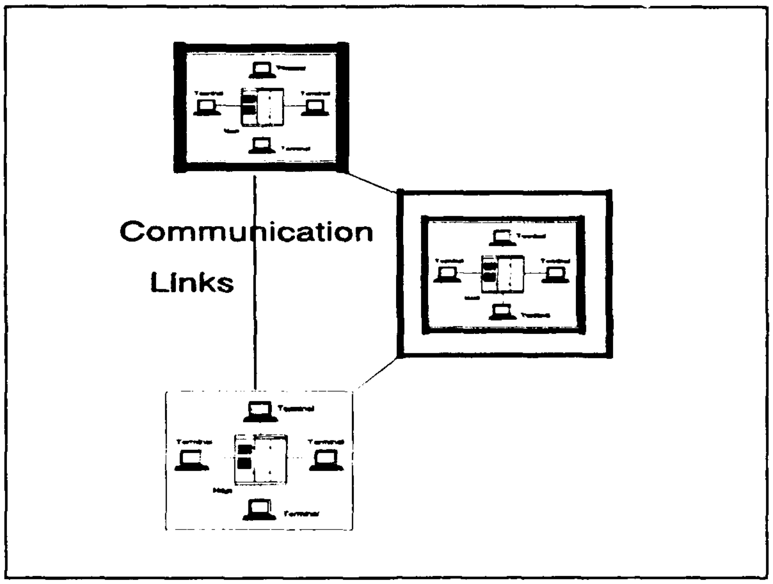

Figure 7 Information is storage and in transit.

Information in transit attacks may be grouped into the general categories of passive and active attacks. (Muftic, 1989; Stallings, 1990)

Passive attacks are designed to disclose information. It may involve content learning where information is observed as it passes through communication channels without altering its contents. Passive attacks may also involve the analysis of message traffic patterns on communication channels by examining the location and identity of users, or message length and frequency. (Stallings, 1990) Traffic analysis can provide valuable information even though the contents of the messages are protected.

Active attacks may involve disclosure, modification, or destruction of information. Message stream modifications results from selectively inserting, replaying, or modifying messages. It may also involve the deletion, delay, and order change of messages. Services may by denied by delay or discard of all the messages.

In general, passive attacks are more difficult to detect but are easier to prevent. Active attacks are easier to detect but are more difficult to counter.

The three most significant threats to telecommunication facilities have remained consistent over the past 75 years. They are people, adverse weather, and accidental destruction of telecommunication facilities. (Menkus, 1990)

- People may misuse facilities by committing unauthorized access or by avoiding the payment of user fees and charges.
- Telecommunication facilities are vulnerable to natural disasters such as floods, ice storms, blizzards, earthquakes, tornadoes, and hurricanes.
- Accidental destruction of telecommunication facility is usually as a result of a fire that affects either the installed telecommunication circuits or the structure in which the switching facility is located. Telecommunication cables strung outdoors on poles are commonly placed along a major highway where they may be struck and damaged.

E. OPPORTUNITY OF THREATS

In comparing threats and assets, the opportunity for a successful attack may be dependent on time. One approach to examining the effect of time is by dividing computer operation into stages. Five stages are presented to indicate possible points of vulnerability. They are: (Bequai, 1983)

1. Input - when information is translated into a language that the computer understands.

2. Output- Often taking the form of thefts of data, customer lists, personnel lists, trade secrets, marketing plans, projected earnings, and other valuable confidential information.

3. Programming - the introduction of the step-by-step instructions for solving the many problems it will later encounter.

4. Usage- Abuse and theft involving the unauthorized use of an employer's computer.

5. Transmission - Transmission of data back and forth between computers or computers and remote terminals.

IV. ANALYSIS OF COUNTERMEASURES

A countermeasure is any action, procedure, technique, device or other measure that reduces the vulnerability of a computer system to the realization of a threat. A vulnerability is a weakness in the protective measures that can be exploited to cause harm or loss. (COMNAVDAC, 1991) An example of a vulnerability is inadequate fire protection. For the purposes of this thesis, the terms countermeasure and control are used interchangeably.

Countermeasures may be conceptualized as performing three basic functions. These functions are prevention, detection and correction of threats. (Bynon, 1990) A particular countermeasure may exhibit more than one of the three basic functions. It may also protect more than one type of asset against more than one type of threat. (Ahituv and Sadan, 1985)

Most countermeasures used in stand-alone systems apply to systems exhibiting a higher degree of distribution. Sometimes they can be applied directly to distributed systems no matter what the degree of distribution. In other cases the application is very different. For purposes of discussion, countermeasures are grouped as follows:

- Organizational controls
- Personnel controls

- Environmental controls
- Physical access controls
- Logical access controls
- Virus controls
- Application development controls
- Communication controls
- Electronic emanation controls
- Contingency planning and backup controls

These controls can be used to meet the security goals unique to distributed systems identified in Chapter I. Methodologies for applying these countermeasures will be reviewed in Chapter V. While the groups of controls could be applied to any information system, distributed or not, the emphasis will be on the application of these controls to the specialized requirements of a distributed environment. (IBM, 1987)

Each system node must assess its own particular needs and practical countermeasures. In large distributed systems, an organization may not be able to dictate policy to other nodes on a network or to common communication carriers. In such cases additional countermeasures must be considered to provide continued system operation. (IBM, 1987)

A. ORGANIZATIONAL CONTROLS

Organizational controls are policies and guidelines established by the highest levels of management. They are strategic in nature in that they dictate policy organization-wide and impact how an information system will be used. It is how management demonstrates its commitment (fulfills its responsibility) to the protection of the organization's information system assets. Examples are the establishment of personnel controls or an asset ownership/responsibility policy.

Management Commitment/Responsibility. The formulation of security policies and procedures shows the commitment of higher level management to security. It also establishes that individuals will be held accountable for security. The designation of a security officer provides a central authority for issues dealing with security. Some functions of this position would be to answer security questions, interpret policy, and make security effective for the distributed system. (Rutledge and Hoffman, 1986)

With increasing degrees of system distribution, the distinction between the traditional data processing person and the traditional user is being lost. Yet, management has a responsibility to its employees and to the organization. It must remove or at least minimize the potential for employees to compromise the system. This includes the responsibility to reduce temptation as well. To fulfill its responsibility management must establish personnel guidelines, which is addressed under personnel controls.

Considerations when establishing organization-wide controls. Organizational controls might apply across several divisions within an organization or across several organizations. When establishing organizational-wide controls, management:

- Must consider organizational culture and different needs.
- Must acknowledge the desire for each organizational entity to set their own standards.
- Identify who is the network (system) administrator.
- Address who defines minimum security requirements.
- Establish a Memorandum Of Agreement (MOA) for multiple organizations connected to the same distributed system.
- Address the problem of connected networks and where differences in protocols, security controls are handled.

Asset Ownership/Responsibility. As assets are moved from centralized systems to distributed systems the responsibility for these assets must move also. Responsibility is assigned for both physical assets and data ownership.

Initiation and implementation of a data ownership program where none exists is not an easy task. Specifically designating responsibility for information is a task much broader than the computer processing area. It may have implications that involve management philosophy, such as how the organization functions, and could influence the reporting structure in the enterprise. (IBM, 1986)

Policy Establishment. Policies should establish periodic audits, password usage, and adequate backup/recovery of distributed system resources. New system standards should include good security program documentation and operational procedures. They should also address source and compiled code library management, complete system specifications, and procedures to check input data for completeness, relevance, and accuracy. (Rutledge and Hoffman, 1986)

Operational Procedures. Operational procedures are an example of organizational controls. They establish procedures for day to day operations on all nodes of the system. Traditional operational controls include such things as controlling errors, supervising error recovery, controlling forms and input/output media.

Beyond selecting reliable system components, management should also implement good problem management techniques and procedures. Procedures for end users to log, monitor and correct errors over a broad geographic area or across organizations must be carefully designed. Unintentional errors by authorized users is already a major problem. The increase in end-user manipulation has the potential to increase these errors. End-users may not be able to recognize or correctly identify problems.

Magnetic media. Magnetic storage media is itself an asset. More importantly, the media is used to hold information assets. Centralized computer facilities develop and enforce rigorous media control policies. These policies address areas such as media marking, storage, destruction, security, and accountability requirements. A list outlining possible policy components is included in Appendix B.

Distributed systems distribute information. The lack of concentrated information storage, particularly for systems comprised of workstations or personal computers, often results in omitting control of magnetic media. Organizational policy must address the value of the media and information assets to select appropriate media controls.

B. PERSONNEL CONTROLS

Personnel controls are classified as a type of organizational controls. Personnel internal to the organization have been identified as the greatest risk group to an information system. It is as an area where management can set policy to enhance the security of the system. These policies may include, for example, segregating duties or establishing criteria for employee selection and retention.

The need. End-user computing is supported with increased distribution. Increased user processing capability also increases their ability to incorrectly process information with no particular checks and balances. It can potentially corrupt databases unless the system is robust enough to withstand the challenges to system integrity. It also increases problems since access by other than select information system (IS) staff involves more than highly controlled operations or requests.

Countermeasures. Personnel should be aware of the value of system assets. The value of information assets is rarely appreciated until it is corrupted or otherwise no longer accessible. To help protect these assets, the following general areas may be considered: (Jackson, 1990)

- Background checks.
- New Employee Indoctrination.
- Statement of Security Responsibility.
- Drug Testing.
- Polygraph Testing.

Some organizations with many distributed processing (DP) assets and networking facilities conduct a pre-employment background check. If an individual is processing critical or sensitive data, a program of periodic background checks is advisable. New employees should be indoctrinated into their responsibilities. Compliance with DP asset protection responsibilities must be mandatory, and should be considered a condition of continued employment. Responsibility must be assigned to the data user, owner, custodian, and management.

The establishment of an employee code of conduct can clearly delineate expected employee responsibility. (IBM, 1986)

The concentration of data within an organization, such as accounting data, is a potential danger because it may allow realization of malicious purposes. Separation of data may not be practical. Satisfactory control can be gained by separating personnel who have access to the data during capture, processing, storing, and retrieval activities. This separation is labeled segregation of duties.

Segregation of duties is a basic principle of internal control. The basic premise of segregation is that once data, processes, or duties are segregated, malicious intent can be realized only through collective efforts. Naturally, such a coordination of employees to exploit the system is difficult to coordinate. Additional segregation of duties can be applied to information systems development and operation activities. (Ahituv and Sadan, 1986)

Because of the nature of network environments, management may want to place more emphasis on and exercise additional controls over job rotation and employee account restriction. Dual responsibility (two person integrity) provides further measures of security. (Rutledge and Hoffman, 1986)

Legal issues. Management must consider the legal issues of personnel policy. For example, monitoring and privacy of electronic mail have been a subject of debate within the legal system. (Bequai, 1983) With end-user computing, employees may develop their own applications. The organization must now consider who owns any patents, copvrights, licenses, and trade secrets. A contract between end-users and the organization can address these issues so that both understand their rights and responsibilities. (Pfleeger, 1989) These policies may be applied over all nodes of a system. The nodes may be distributed over a broad geographic area, each with its own culture or legal system.

C. ENVIRONMENTAL CONTROLS

Environmental threats as a group are the most visible and tangible threats. They can also be the most devastating. Accordingly, management is most often willing to commit resources to control these threats. As the distributed system extends across organizational, sites the chance for fire, water, and natural disaster damage increase. Environmental protection must satisfy two objectives: preservation of physical assets and system availability. Most of the security measures used for the computer center need to be carried over into distributed systems. (Rutledge and Hoffman, 1986) The following environmental controls are primarily oriented to the protection of building and facilities. (IBM, 1987)

Air conditioning. Air conditioning is employed to maintain temperature and humidity within system operating parameters. Large computing centers require special air conditioning equipment to meet stringent requirements.

Distributed system nodes such as work stations or intelligent terminals are designed to operate in office environments. If continued system operation is needed in the event of facility air condition system failure, consideration should be made for the installation of a backup system.

Electrical power controls. Electrical power controls protect systems against power supply outages and fluctuations. Some common mechanisms are line conditioners, uninterruptible power supply (UPS) systems, and backup electric generators. (King, 1990) Both line conditioners and UPS systems filter commercial power by absorbing fluctuations and ensuri g clean ele trical power. UPS will also continue to supply electricity for a short time to safely operate equipment. During this period other backup power sources are invoked or equipment is shut off. Backup electric generators can be used not only to provide power to data processing equipment, but to other essential services such as lighting, chilled water, and air-conditioning systems. The high cost of installation and maintenance of these countermeasures, particularly for backup electric generators, must be justified by the degree of dependency of the data processing operations. (Jackson, 1990)

Water. Computer systems are both dependent on and adversely effected by water. Water is used for cooling either through air conditioning or system components themselves. An interruption in supply normally leads to the system exceeding safe operating conditions. Undesired events such as leaks in plumbing, air-conditioning, chilled water, or fire suppression systems must be anticipated. Thought should also be given to roof integrity, integrity, and under floor drainage capabilities. Prefitted waterproof covers or simple plastic sheeting located in equipment rooms is a valuable countermeasure should water leakage occur. (Jackson, 1990)

Lighting. The degree of lighting requirements within a particular facility is dependent on the need for continued operation in the event of power failure. If continued operation is needed, then the power requirements for adequate lighting must be considered when selecting backup power system capacity.

Fire controls. Centralized computing facilities use a variety of fire detection and suppression techniques. Distributed system components, often located in office buildings, are partially protected by fire detection and automatic fire suppression systems normally required for such facilities. (King, 1990) The value of the equipment in any particular location will dictate whether it is economically feasible to install dedicated automatic systems that use CO_2 or Halon. Portable fire extinguishers are an excellent first line of defense in keeping small fires from spreading. Clearly labeled and visible extinguishers should be placed in centralized computer rooms, tape and disks storage areas, form storage, and any other auxiliary machine rooms within the facility. (Jackson, 1990)

Housekeeping. In a traditional centralized facility housekeeping measures emphasizes cleanliness and minimal flammable material (paper) storage within or near the computer room to reduce the risk of fire. Distributed system nodes within office spaces makes this approach difficult to implement. Where waste paper accumulates the use of self extinguishing waste paper containers can be effective in reducing the fire threat. (Jackson, 1990)

D. PHYSICAL ACCESS CONTROLS

Physical access controls involve limiting access to system assets such as hardware, storage media, and documentation. End-user computing supported by distributed systems necessitates increased access to system assets while the assets themselves are spread over a broad geographic area. These controls strive to allow authorized personnel access without excessive effort.

The implementation of physical access controls must include the identification of areas where they may be practiced. Some possible areas unique to distributed systems are: (IBM, 1987)

- Remote facilities whether located in the same building or in another site.
- Communication link components.

- Common-carrier-provided equipment, links, and facilities through which organizational data must be transmitted.
- Network control center facilities that normally house all of the specialized network equipment for patching, monitoring, and testing network components.
- Information center facilities that have been established as the focal points for helping end-users in the design and implementation of specialized department applications.
- User required materials like operations manuals, floppy disks, and copies of licensed vendor supplied software.
- Shared remote printer output areas.

The centralized system approach to physical access controls emphasizes the placement of computer resources in limited access areas. This approach segregates assets such as computers, peripherals, removable secondary storage media and personnel. Distributed systems move assets into environments such as offices where limiting access to all components is neither practical or desirable. In these cases additional measures such as securing cables and locks on pilferable items provides added security. (Jackson, 1990)

Unauthorized physical access requires knowledge of the asset's existence. The visibility of critical system components must be limited. Avoid advertising the location of assets such as wiring closets or network file servers with external markings or signs. (Jackson, 1990)

The required complexity of physical access controls can depend on the size of the organization and hours of operation at any particular node of the system. For small organizations simple measures may be appropriate since an unauthorized individual would be easily recognized. In larger organizations this approach is not practical and would require more formalized controls. Some methods that restrict access include: (McNurlin and Sprague, 1989)

- Having a receptionist monitor access at the office entrance.
- Using badges and color codes on badges to indicate authorization.
- Signing passes for taking assets in and out of the facility.

After working hours, physical access can be further restricted since authorized user activity is low. Some heightened measures include locking doors and windows, having adequate night lights, and hiring a security service. While not authorized users, janitorial services are active after hours and require access to perform their functions. Of particular concern are the procedures used by the janitorial service. Though convenient to the janitors, unlocking several doors provides the opportunity for unauthorized personnel to gain access. The effective control of keys is an important part of physical access controls. (McNurlin and Sprague, 1989)

E. LOGICAL ACCESS CONTROLS

Access controls provide for the prevention of unauthorized use of assets. Unauthorized use includes the use of an asset in an unauthorized manner. (COMNAVDAC, 1991) Access privileges are a function of three basic components. These components are defined as: (NCSC, 1987)

- Subjects. An active entity, generally a person, process, or device that causes information to flow among objects or changes the system state.
- Objects. A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, etc., (network resources) access rights (entry privileges).
- Conditions for resource usage.

By manipulating these three basic components, access control limits the rights or capabilities of a subject to communicate with other subjects. They can also limit access to functions or services within a computer system or network. (NCSC, 1987)

Mechanisms providing logical access control may be structured in the form of lists, a matrix, a binary tree, or a more general hierarchical structure. In any form, access control mechanisms must contain information necessary to provide controlled access to network assets. (Muftic, 1989)

Logical Segmentation. Logical access performs two types of segmentation. The first is the identification and verification of authorized users. The second is to limit authorized users access to only those resources required to accomplish assigned job functions.(IBM, 1987)

Placing a value on information often facilitates grouping the information into classes. Multiple classes of information can be processed within or across several nodes of a system. The method of limiting access to resources by segregation must be part of the security plan. Five possible modes of system operation based on the classification(s) of information and access allowed are: partitioned, dedicated, multilevel, system high, and limited access. These modes of operation dictate the type of segregation employed and are defined as: (NCSC, 1987)

- Partitioned. A mode of operation wherein all personnel have the clearance, but not necessarily a formal access approval and need-to-know, for all information handled by the system.

- Dedicated. The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type of classification of information, either for full-time operation or for a specific period of time.

- Multilevel. The mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present.

- System High. The mode of operation in which system hardware and software is only trusted to provide discretionary protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and / or stored. All system users in this environment must possess clearances and authorization for all information contained in the system. All system output must be clearly marked with the highest classification until the information h's been reviewed manually by an authorized individual to ensure appropriate classification and that caveats have been affixed.

- Limited Access. A mode of operation relating to unclassified data only, clearances are not required, but access is restricted to users with need-to-know. The control is provided by special access controls such as read/write keys, user Ids and passwords.

These modes of operation are applicable to all systems no matter what the degree of system distribution. It is the mechanism to implement the mode of operation that becomes more complex as the degree of distribution increases.

Distributed system design should include sufficient controls to defend themselves against access threats. Unfortunately, most systems are not considered sufficiently trustworthy to do so. Information systems not trusted to segregate information of various classification levels operate in the dedicated or system high mode. In such operation, all authorized users must have security clearances appropriate for the highest classification of data on the system though actual access may not include all system objects. Output from these systems is protected as though it contains the most highly classified information. Output must be reliably reviewed and its actual classification and sensitivity verified. (Neugent, 1989)

Centralized/Distributed Control. Two basic designs exist for network logical access controls. Centralized access control involves a centrally managed and controlled network monitoring and security system. A particular location or node provides system wide:

- Access authorization management.
- Issuance of user identification.
- Password management.
- Audit trail management.

Under distributed access control, each node independently handles such requirements though a frequent information exchange process. Users having gained access on one node normally are accepted on other nodes of the system. Larger systems tend to employ architectures that are a combination of the two. (Lace, 1990; Browne, 1984)

Effect of topology. The network topology determines how interconnect schemes will influence the ability to secure data. (Lace, 1990) An important factor in deciding on how to implement logical access control in a distributed environment is the topology of the system. The hierarchical or star topology favors central control. A star topology or hierarchical interconnect topology offers the best security control because the control can be centralized or constructed modularly.

Other topologies favors distributed control and are characterized by a lack of an identifiable centralized node to provide access controls to the network. Architectures such as ring, mesh, or bus topologies, tend to disperse the control to individual nodes. These topologies rely on exchanges of information to maintain system integrity and security. (Lace, 1990)

Centralized control suffers in performance since all requests must first be passed to, processed by, and returned from the central node. Administrative overhead grows as the degree of access control increases, and as the system size increases. Distributed network control is weak in security policy enforcement. This deficiency stems from different security attributes available on each node. For example, data that is weakly protected on one node could be sent to another node, altered, and returned to the original without the originator knowing that this occurred. Thus, data integrity can be easily compromised unless detection and subsequent countermeasures are implemented. These measures could include host or user alternatives, such as port protection devices, and encryption/decryption devices. (Lace, 1990)

Implementation. Implementation of logical access controls requires invoking good administrative procedures. These procedures must first identify the resources to be protected. They must identify each individual in the organization with a unique user identifier. Lastly, they must provide an authentication capability to verify that a user is really who he or she claims to be. These procedures may be accomplished by having each user represented to the system by:

- What the user knows - passwords.
- What the user has - magnetic card or token.
- What the user is - biometrics such as fingerprints, signatures, retinal scans.

They may also be accomplished by providing an authorization scheme by which the resource owner has the responsibility:

- To identify the users or user groups who may access the protected resources.
- To identify the access authorization to be granted and assigning to each individual user or user group.
- Of recording resource utilization.
- Of taking appropriate management action to correct variances to normal behavior and to prevent future occurrences of violations.

F. VIRUS CONTROLS

Virus is defined as "Code that covertly replicates itself onto previously uncontaminated media without initiation by the operator of authorized users." (SECNAVINST, 1989) Replication usually occurs during copying of files to magnetic media, or during computer to computer communications. The code usually contains malicious logic that is triggered by some predetermined event. When triggered, the code then takes a hostile action against host computer systems.

The issues surrounding malicious software such as computer virus are intriguing. It is important not to overlook the fact that they are created by people. Hence, computer virus can be addressed a personnel problem. A virus is a tool used by people to extend and enhance their ability to create mischief and damage. Malicious software exploits the same vulnerabilities as can knowledgeable users. Thus, any steps taken to reduce the likelihood of attack by malicious software should address the likelihood of unauthorized use by computer users. (NIST, 1987)

Controls based on system size. A distinction may be made between multiuser computers with associated networks and personal computers (workstations) with associated networks. (NIST, 1987) Virus prevention differs mainly in the following two respects:

- The relative lack of technical controls.
- The resultant emphasis this places on less technically oriented means of protection which necessitates more reliance on user involvement.

Distributed systems based on personal computers or workstations typically do not provide technical control for such things as user authentication, access control, or memory protection that differentiates between system memory and memory used by user applications. The lack of controls permits users to share and modify software. Thus, small computer based systems are more prone to attack by viruses, unauthorized users, and related threats. (NIST, 1987)

Regardless of the size of the system, the following groups of efforts are useful in combating virus threats: (NIST, 1987)

- General policies.
- Software management.
- Technical controls.
- Monitoring and audit trails.
- Contingency planning.

Controls based on the degree of distribution. Virus prevention in the multiuser computer environment is aided by the centralized system and user management, and the relative richness of technical controls. Unlike personal computers, many multiuser systems possess basic controls for user authentication, for levels of access to files and directories, and for protected regions of memory. These controls are not adequate by themselves. Distributed systems can greatly reduce their vulnerabilities to attack when combined with other policies and procedures that specifically target viruses and related threats. (NIST, 1987)

Types of controls. There are a number of different controls which can be implemented to prevent viruses or detect those that exist: (Phillips, 1990)

- Use a "virus antibiotic program" on all new software.
- Isolate new software until it is tested.
- Know the origin of all software, don't use unsealed software from unknown sources.

- Be wary of download software, especially from public bulletin boards.

- Don't let anyone put anything on a machine without authorization.

- Periodically check for reinfection.

- Use file/program checksum.

- Compare the length of programs regularly.

- When ever possible, boot from the hard disk, not a diskette.

- For diskette-only computers, always boot from the same write-protected diskette made from an original system diskette.

- Find and remove extraneous command.com copies from the hard disk.

- Use type domain mechanisms.

- Ensure proper password use.

- Use trusted system operating systems.

- Ensure purchased commercial software is in its original shrink-wrapping.

- Buy software only from reputable sources.

- Restrict access to systems programs and data on a need-to-know basis.

- Put software on CD-ROM.

- Backup your data files regularly.

- Write protect executable files.

- Encrypt executable files.

- Monitor the modification dates of programs and files.

- Use removable hard disks.

- On a hard disk system, never boot from an "imported" floppy.

- Do not keep diskettes inserted unless actively in use.
- Inoculate program files with commercially available virus protection software.
- Look for changes in volume labels.
- Run suspect programs on unimportant diskettes.
- Watch for changes in a systems's operation.
- Clear memory before and after running a confidential program.
- Forbid employees to install unauthorized software on office computers or to take office software home for use.
- Never attempt to isolate or remove a virus from a currently active computer. Boot from a "clean" diskette.
- Remove from service all copies of a suspect program and immediately back up all related data.

G. APPLICATION DEVELOPMENT CONTROLS

Application development controls are a set of procedures to guide the development and maintenance of software used to store, manipulate, or communicate the organization's information assets. End-user involvement in application development has placed new demands on the process. Some of these demands are:

- Greater demands of features, performance, flexibility.
- Demand greater involvement in the development process.
- Their acceptance of new systems more important.
- May need to operate on different systems (hardware or operating systems) attached to the network.

Though satisfying immediate end-user demands, the localized development of applications can lead to incompatible data. The close coupling of data to specific applications result in isolated islands of data.

Countermeasures. Traditional application development controls consist of steps such as project phase reviews under a project control system, establishing standards, controlling changes, quality control, and library content control. Improved programming technology techniques like structured programming enhance software portability and maintainability. The auditing of applications to a set of expectations is also beneficial in maintaining compatibility across a distributed system.

Organizations that choose to implement a distributed approach to applications development should also be prepared to support the new environment. Some items which should be considered for inclusion in guidelines are:

- Acquiring only authorized software that meets organizational needs.
- Documentation requirements for locally-developed code.
- Rigorous change procedures.
- Downloading of object code only from the host.
- Testing and integration procedures for new applications.
- Data backup and migration practices.
- Documentation requirements for operation of the application.

- Requirements for logging application events.
- Requirements for data integrity.
- Requirements for auditing application results.
- Requirements for logging of input/output errors.
- Requirements for fault isolation and resolution.

H. COMMUNICATION CONTROLS

Distributed systems is defined in Chapter I by the presence of electronic communications between multiple nodes of a system. Telecommunications is identified in Chapter III as inherently insecure. (Menkus, 1990) The implementation of controls designed to protect communications is essential to maintain the integrity of a distributed system. Two groups of controls will be examined. They are cryptographic and dial-up controls.

The telecommunication process involves an origin, a destination, and the intervening transmission. Transmission is the aspect of telecommunications where the inherent weakness in most data communications security processes is to be found. Transmission is the most complex and unpredictable aspect of telecommunications. It is the unpredictability that created the weakness. (Menkus, 1990)

Communications Security Approaches. All communications controls are classified as providing link oriented or end-to-end oriented services. Link oriented controls protect information in transit on each discrete communication link between nodes. End-to-end controls protect information in transit from its source to its destination. These two approaches are implemented differently and provide different security services. (Rutledge and Hoffman, 1986)

Cryptography. Cryptography involves rendering plain text unintelligible and for converting encrypted text into intelligible text. The implementation of cryptographic controls may be implemented in several ways. Some examples are:

- Link encryption. One physical communication link is protected by installing cryptographic devices on each end of the communications link.
- Integrated cryptography. The node's operating system controls the capacity to selectively encrypt information before transmission.
- Application Software. Application software controls the capacity to encrypt information.

Cryptographic controls have two major limitations. First, encrypted information protection is limited to content disclosure. It is best used as a supplemental control to defeat disclosure of information threats for information both in transmission and in storage. Secondly, effectiveness of cryptography is based on the quality of the selected encryption algorithm, cipher key generation, and cipher key protection. (IBM, 1986)

Cryptography may be used as both a link oriented control and an end-to-end oriented control in communications security. Link encryption requires each vulnerable communications link to be equipped on both ends with an encryption device. Both the information and system routing instructions are protected from contents disclosure during transmission. However, the information is vulnerable to disclosure within any intermediate node of the distributed system. (Stallings, 1990)

End-to-end encryption involves the source encrypting the information that is transmitted across the distributed system. Since intermediate nodes may be involved, system routing information cannot be encrypted. The destination decrypts the information data by using a shared key. This approach protects the information from content disclosure both during transmission and while in any intermediate node but still suffers limitations. While information is safe from disclosure, the traffic pattern is not.

Limitations of link oriented or end-to-end oriented cryptography may prevent either of the schemes from providing adequate protection. Security requirements may be better met by the combined use of these two schemes. By employing both forms of encryption, the origin encrypts the information to be transmitted using end-to-end encryption. During transmission link encryption is employed for each vulnerable communication link. Thus, during transmission the entire message is protected from disclosure. At any intermediate node, only the system routing information is available, the remainder being protected by the end-to-end encryption.

Dial Up Controls. The ability to remotely access information systems increases system connectivity for the organization. Dial up ports can be accessed from anywhere in the world that is supported by common telephone networks. A system's dial up ports, regardless of the degree of distribution, present a major access point to the system where threats may attack. In addition to the physical access mechanism, controls such as logical access must be employed to maintain system integrity. (Troy, 1985)

Dial-up controls are based on three primary functions. They are identification, audit trail, and brute force attack limits. User identification and authentication are the cornerstone of access controls. Audit trails are useful in identifying user difficulties and attempted intrusions. Brute force attack limits act by controlling the number of access attempts per connection session. These functions may be provided by node or network operating systems. External devices may also be employed if the systems are not capable of providing these functions. (Troy, 1985)

The actual implementation of dial up controls can be at one or both ends of a potential communication link involving dial up ports. One-ended protection approaches for dial up communications security employ controls at the host computer's port. Port protection devices (PPD) are external to the system and perform services before and independent of the system's own access control functions. Primary features of a PPD include: (Troy, 1985)

- Password tables. Provides password based access protection for the computer's ports independent of any potential system password access control.
- Dial-back to call originator. Provides a second level of user or port authentication beyond the standard PPD password table. A typical connection attempt might involve a user accessing the PPD and entering a password. The PPD ends the connection and validates the user. The PPD then returns a call to a predetermined number associated with the given password to establish a communications session.
- Hiding the port's existence. Several approaches may be used to mask the port against accidental discovery of the port's existence. They include user terminal screen displays that are initially blank or ambiguous, require user knowledge of procedures to gain access to the system, or even response by synthesized voice.
- Audit trail of connection events. Provides the system administrator to review both user difficulties and unsuccessful attempts to access the port.

Two-ended protection approaches for additional dial-up communication security may be employed when more positive identification of the specific terminal or user may be needed. The two-ended approach uses a device or software on each end of the communications link. These devices use complex algorithms uniquely associated with specific terminals or users. For user convenience algorithms may be embedded into integrated circuit chips encased in some form of "token" such as a plastic card. Others are embedded in the circuitry of system components providing communications services. This approach avoids the user having to remember passwords. The added protection provided by two-ended protection devices to the dial-up communications network, however, must be justified against increased cost. (Troy, 1985)

Backup telecommunication services. To ensure availability of critical communications services organizations typically employ two different approaches. The first is to acquire duplicate communications facilities. The second is to use alternate communications technologies that can be deployed in an emergency. Either of these approaches may be implemented by direct acquisition or as services provided by organizations that specialize in providing backup communications mechanisms. (McNurlin and Sprague, 1989)

I. ELECTRONIC EMANATION CONTROLS

Electronic emanations are signals transmitted as radiation through the air and conductors. Emanations security controls are measures designed to deny unauthorized access to information that might be derived from intercept and analysis of compromising emanations. This threat leads the United States Government to develop the TEMPEST (Transient ElectroMagnetic Pulse Emanation STandard) program and related technology. (COMNAVDAC, 1991) Due to cost and rigorous program requirements, TEMPEST technology is used primarily to protect classified information. Federal government, military, and defense contractors are the primarily users. (Jackson, 1990)

Two traditional approaches are taken to prevent disclosure through emanations. The first employs shielding system components or entire computing facilities to trap signals. The second is the modification of emitted signals such as the addition of spurious signals. Through shielding or modification of the emanations, adversaries are prevented from intercepting and interpreting electromagnetic emanations from computers, communications devices, and other electronic equipment. (Jackson, 1990)

Electronic communications used by distributed systems complicates emanations security. Wire communications media are subject to passive wiretapping. Microwave signals are transmitted through the air, and are susceptible to monitoring anywhere along the signal path. Satellite communications pose even greater potential for interception. In each case the volume of information transmitted makes separation of individual transmissions difficult. Link or end-to-end oriented communications controls provide additional assurances of maintaining system integrity.

J. CONTINGENCY PLANNING AND BACKUP CONTROLS

Contingency planning and backup controls are frequently included as part of organizational controls. A list outlining components of contingency plans is included in Appendix C.

These plans must address actions to be taken if processing centers or support facilities were to face a catastrophic event. Management must recognize that centralizing processing into one or a few centers may be a high security risk. If a successful threat attack wipes out a centralized facility, the organization could suffer losses even when provisions have been made for a backup center. (McNurlin and Sprague, 1989)

Distributed systems increase the total risk an organization faces. Yet, its geographically dispersed nodes and electronic connection also provides a unique countermeasure to avoid catastrophes. Multiple nodes present in distributed systems can provide higher overall reliability and availability than centralized mainframes.

Organizations which use distributed systems as part of their disaster recovery program perform critical processing functions locally rather than centrally. The distribution of processing permits operations to continue uninterrupted at all other nodes of the system when one is successfully attacked.

Hardware and application selection to these organizations becomes critical. Often they are standardized so that each node is capable of serving as a substitute for any other node. The arrival of industry open system architectures and families of compatible systems has helped to lessen this requirement. The cost of security by redundancy must be viewed against the criticality of any particular process or information. (McNurlin and Sprague, 1989)

V. SECURING DISTRIBUTED SYSTEMS

Commitment by organizational management is critical for the success of a computer security program (Powell, 1990). Management must be made aware of the impact of threats against the organization's assets such as compromise of national security, media attention, monetary loss, or legal liability (Wood, 1990). There are two elements in managing computer security. They are:

- Risk Management.
- Developing a security plan.

Figure 8 displays a general model of protecting assets from threats. The importance of any particular layer of controls (identified in Chapter IV) is dependent on the particular environment in which a distributed system exists. In this model, system assets are protected by the cumulative efforts of all controls implemented.

Another model, depicted in Figure 9, is based on the functionality of controls displaying the relationship between threats, vulnerabilities, and assets.

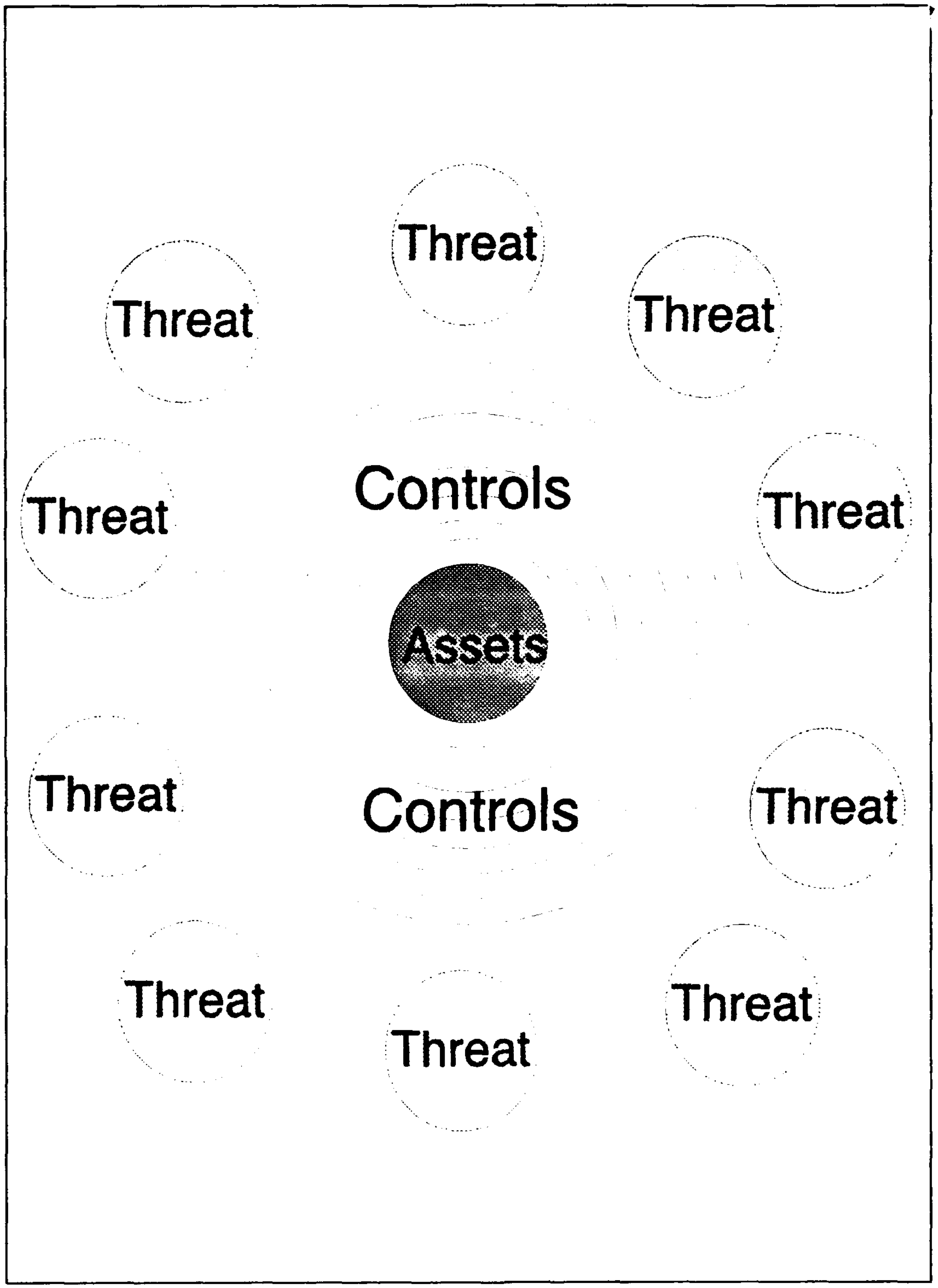

Figure 8 General model of threats, assets, and controls.

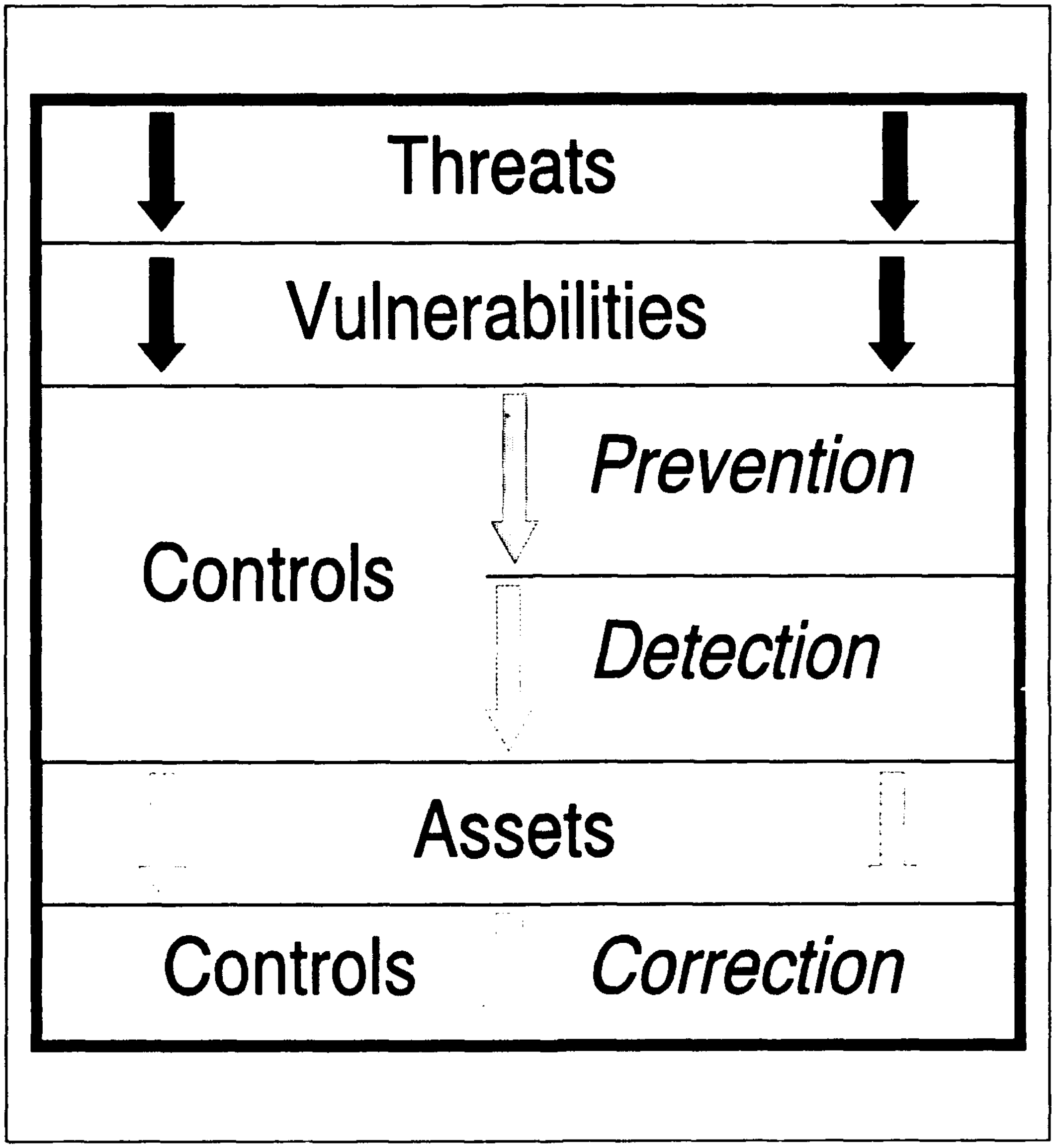

Figure 9 Functionality of controls.

A. RISK MANAGEMENT AND SECURITY PLAN

Risk management may be either qualitative or quantitative. (Palmer, 1990) There are four strategies when addressing risk control. They are (Pfleeger, 1989):

- Risk avoidance. Avoid or prevent loss.
- Risk reduction. Minimize the potential for successful attack.
- Risk transfer. Move critical functions to systems already protected.
- Live with it. Risk acceptance with a contingency plan in event of successful attack.

Applied to distributed systems, risk management is the process of identifying, measuring, and minimizing uncertain events affecting system assets. Risks can differ greatly from one organization to another depending on its activities. (IBM, 1987) Even within an organization, different nodes of a distributed system may exist in unique environments and require individual attention. Risk management includes the following functions: (COMNAVDAC, 1991)

- Risk analysis.
- Cost benefit analysis.
- Safeguard selection.
- Security test & evaluation.
- Contingency planning.
- Systems reviews.

The purpose of risk analysis is to establish and maintain the most cost effective controls which provide an acceptable level of security. It is an orderly process rooted in management practices. Reasons to perform risk analysis identified by (Pfleeger, 1989) are:

- Improved security awareness.
- Identify existing assets, vulnerabilities, and controls.
- Improved basis for decisions.
- Justify expenditures for security.

Several different schemes exist for performing risk analysis. Each scheme follows the same basic steps. These steps identified by (Pfleeger, 1989) are:

- Identify assets.
- Determine vulnerabilities.
- Estimate likelihood of exploitation.
- Compute expected annual loss.
- Survey application controls and their costs.
- Project annual savings of control.

The selection of possible controls should involve more than just a cost benefit analysis. The feasibility of each control may be determined by examining three factors. These three factors are economic feasibility, technical feasibility, and operational feasibility. (Browne, 1979)

- Economic feasibility. Traditional cost 'enefit analysis of the value gained by the organization from the control against the cost of implementing the control.

- Technical feasibility. An organization must possess the technical capability to manage the control. Industry must possess the technical capability to provide and maintain the control.

- Operational feasibility. How the control will influence the operation of the organization.

Different nodes of a distributed system may select different controls for the same threats against identical assets based on these three factors.

Risk analysis is the study of the risk of some action. It is the first step in identifying threats, assets, and controls for any system. The risk analysis results are then used as the basis for developing a comprehensive security program.

A security plan is a comprehensive guide of an organization's security activities. The plan is both a description of the organization's current security posture and blueprint for change. (Bynon, 1990) It is an organization-wide policy statement by the highest levels of management. This policy sets the overall goals and provides a set of benchmarks for measuring achievement. Supporting documents and instructions provide more detailed and environment specific objectives. Yet, many security "plans" are a collection of controls added on a piecemeal basis without consideration for the overall threat. (Browne, 1979; IBM, 1987)

The contents of a security plan is specific for a particular organization as it expresses its goals. A security plan must also be justifiable in terms of cost and potential impact on the organization. (Tate, 1988) A simple return on investment approach may not fully identify benefits derived from a security program. Consideration must be given to less tangible services such as the integrity of information used by management to make decisions. A comprehensive plan can also be used to an organization's competitive advantage such as increasing customer confidence. (Wood, 1991) The plan is subject to periodic review and revision as the security needs of the organization change. (Jackson, 1990) General areas that every security plan must address are: (Pfleeger, 1989; Bynon, 1990; Stephenson, 1991)

- Policy. A statement indicating the goals of a computer security effort and the willingness of personnel to work to achieve those goals.
- Current state. A description of the status of security at the time of the plan.
- Recommendations. Steps that will lead to meeting the security goals identified previously.
- Accountability. A listing describing who is responsible for each security activity.
- Timetable. A record identifying when different security functions are to be done.
- Continuing attention. A statement specifying a structure for periodic review and revision of the security plan.

When establishing a security plan, select those items identified under risk management which provide the greatest visible benefit for the least cost. Initial success of the plan will bolster management support. As the organization matures in its security posture, less overt emphasis on security will be required. General awareness of security issues become integral in corporate culture.

B. TRUSTED COMPUTER BASE (TCB)

The Department of Defense (DOD) has played a lead role in the evolution of computer security. Six underlying requirements have directed DOD efforts in secure computer systems. They are identified (NCSC, 1985) as:

- Security policy. There must be an explicit and well-defined security policy enforced by the system.
- Identification. Every subject must be uniquely and convincingly identified. Identification is necessary so that subject/object access request can be checked.
- Marking. Every object must be associated with a "label" that indicates the security level of the object. The association, which is also known as "marking" the object, must be done so that the label is available for comparison each time an access to the object is requested.
- Accountability. The system must maintain complete, secure records of actions that affect security. Such actions include introduction of new users to the system, assignment or change of the security level of a subject or an object, and denied access attempts.
- Assurance. The computing system must contain mechanisms that enforce security, and it must be possible to evaluate the effectiveness of these mechanisms.

- Continuous protection. The mechanism that implement security must be protected against unauthorized change.

Based on these six requirements, the DOD has developed a set of theoretically based standards. They define levels of information security in terms of function and assurance. These standards are published in the document called Trusted Computer System Evaluation Criteria, TCSEC, otherwise known as "The Orange Book" (DOD-5200.28-STD). (Lorin, 1988) The level of trust required by specific system environments is described in the "Computer Security Requirements -- Guide for Applying the DOD TCSEC in Specific Environments" (CSC-STD-003-85).

The private sector has become more concerned as a result of increased instances of computer intrusion. As the DOD, the private sector has become increasingly dependent on information processing assets. Any increase in dependency on any particular asset increases the potential impact of that asset being attacked. It has also been pressured by the government for the concern that private-sector data represents a national resource. Fifteen factors driving the civilian computer security market are identified by Wood (1990). They are:

- Media attention.
- External auditor comments.
- Insurance premium rating.
- Information system expenditures.

- Personal liability.
- Government laws and regulations.
- Military research.
- Elastic demand curve.
- New technologies outstrip controls.
- System interconnection.
- System integration.
- Distributed data processing.
- Computer literacy.
- Commodity platforms.
- Security standards.

Most large general purpose information systems, including distributed systems, support multiple subjects (users) accessing multiple levels of object (data) classification. Strict limits on users access rights must be defined. Further, there must be no method for violating these limits. (Lorin, 1988)

The alternative to multi-subject, multi-level object systems is the employment of dedicated systems for each level of information classification. The premise of this scheme is physical isolation to improve information security. This scheme becomes unmanageable for large systems where it would result in the proliferation individual systems and associated assets. While the information held on any one system may be more secure, the overall organization is less secure because larger populations must be trusted. The interconnection of computers makes the concept of physical security at a single system inadequate to address the security issue. (Lorin, 1988)

Some researchers extending TCSEC to trusted distributed systems maintain that there is little intrinsic difference in the assurances required from a trusted stand-alone system. In each case, access control policy dictates all allowed access between each subject and each object on the system. Formal verification is used to provide assurance about system compliance to the access control policy (Schaefer, 1985). Other researchers feel that a disproportionate amount of effort is placed in ensuring access control of classified data while not properly addressing information integrity. (Clark and Wilson, 1990)

TCSEC has been formally extended to distributed systems by the DOD National Computer Security Center (NCSC). The ensuing document is called Trusted Network Interpretation (TNI), otherwise known as "The Red Book". TNI uses the term network to represent all types of distributed systems. Accreditation is the managerial authorization to operate a system which has been proven to be in compliance with TCSEC requirements. TNI recognizes two means of accrediting networks. Systems can be viewed as a collection of independent nodes which are created, managed, and accredited through a joint approval process. Alternatively, a network can be treated as a single system and accredited as a single entity. (Lance, 1990)

Through interpreting the TCSEC for networks, TNI contains all of the criteria in the TCSEC and adds rationale to applying trust technology to netwcrk systems. As with TCSEC itself, the interpretation has been prepared to provide guidance over three areas. As listed in the TNI they are:

- To provide a standard to manufacturers as to what security features and assurance levels to build into their new and planned, commercial network products in order to provide widely available systems that satisfy trusted requirements for sensitive applications.
- To provide a metric by which to evaluate the degree of trust that can be placed in a given network system for processing sensitive information.
- To provide a basis for specifying security requirements in acquisition specifications.

TNI is presented in two parts. Part I is the direct interpretation of TCSEC for network systems. The specific security features, assurance requirements, and the rating structure of the TCSEC are extended to networks of computers ranging from isolated local area networks to wide-area internetwork systems. The primary emphasis of Part I, as TCSEC, is controlling access to information.

The procedure for determining the minimum security requirements for a network parallels the procedure for a stand-alone system. The procedure for computing the risk index contains six major steps (DODD 5200.28 Enclosure (4)). These steps are listed as:

1. Determine system security mode of operation.

2. Determine minimum user clearance or authorization rating.

3. Determine maximum data sensitivity rating.

4. Determine risk index.

5. Determine minimum security evaluation class for computer-based controls.

6. Determine adjustments to computer security evaluation class required.

The risk index is used to determine which NCSC-evaluation ratings is required of the system to provide adequate security as minimum requirements.

TNI Part II contains additional network security concerns such as communications integrity, denial of service, and transmission security. TNI Part I does not describe all the security requirements that may be imposed on a network. Depending upon the particular environment, other measures may be required. Examples of the functionality of security services are (NCSC, 1990):

- Authentication.
- Communications field integrity.
- Non-repudiation.
- Denial of service.
- Protocol based DOS protection.
- Network management.
- Data confidentiality.
- Traffic flow confidentiality.
- Selective routing.

These concerns differentiate the network environment from the stand-alone computer. Some concerns take on increased significance in the network environment while others do not exist on stand-alone computers. Many are outside the scope of Part I or lack theoretical and formal analysis. The criteria in this Part II addresses these concerns as additional security requirements that may vary among applications.

TNI Part II security requirements describe qualitative evaluations of security services in terms of functionality, strength of mechanism, and assurance. The fact that Part II services have not been supported by equally well developed theories and detailed evaluation criteria should not be interpreted to imply that their security problems do not have to be evaluated as rigorously as TNI Part I.

The *Trusted Network Interpretation* (TNI) Environments Guide (TNIEG) addresses many issues needed to achieve the level of trust required in different network environments. It complements the TNI, just as the Trusted Computer System Evaluation Criteria (TCSEC) Environments Guide complements the TCSEC. It is an evolving document which advances as technology and experience is gained in implementing trusted networks. This document applies to networks that are entrusted with the processing of information, regardless of whether that information is classified, sensitive, or otherwise relevant to national security.

VI. CONCLUSIONS AND RECOMMENDATIONS

The primary research focus was on identifying aspects of computer security unique to distributed systems. This study was designed to help managers gain an appreciation for security issues faced in distributed environments. Security goals related to distributed systems were identified in Chapter I. These goals were derived from a wide range of literature sources. These must be combined with other objectives applicable to stand-alone systems to achieve an overall security plan.

It is interesting to note strong similarity between the security goals listed in Chapter I and goals of the highly formalized TCSEC security program. It is also interesting to compare the impact of organizational culture on the implementation of security programs. Vast differences are seen in the actual security programs stemming from similar goals.

Characteristics of distributed systems are and why they differ from stand-alone systems were introduced in Chapter II. The differences were the underlying causes of the security goals posed in Chapter I.

Chapter III assisted in identifying system assets. A list of possible assets is provided in Appendix A. It also discussed the nature of threats to systems which possess characteristics associated with distributed systems. Chapter IV covered a broad scope of countermeasures which may be used to protect distributed systems. It provides the basic tools used in securing distributed processing. Again, this was not a complete list, but rather focused on those countermeasures applicable to distributed systems.

The general mechanism to secure distributed systems was outlined in Chapter V. This approach involved risk management and developing a security plan. There is no optimal solution to designing a security system for a distributed system. The level of security depends on the perceived threats and the risks in a particular environment. The environment faces by distributed systems can be much more diverse than stand-alone systems. Risk assessment is required to evaluate and select security measures. Yet the impact of these controls must be considered against the objectives and operating practices of the organization. A balance must be established between tight controls which may adversely impact operations of the organization against loose controls which result in security problems. As an example of a security program, the DOD's highly structured and theoretically researched TCSEC is presented for evaluation.

Regardless of the complexity of the network environment, security remains a management issue, not a technological one. Prudent management, therefore, will take advantage of the knowledge that the potential for loss in a network environment is greater that in any other. They must implement a security plan in advance of installing a distributed system and review the specific controls as the system expands. It is a matter for management to design a security plan that applies to their unique organization. Management must then emphasize the need to abide by their plan throughout the organization, and follow it up to ensure that the plan is invoked as prescribed.

APPENDIX A (INFORMATION SYSTEMS ASSETS)

Eight Asset Categories:

1. Hardware
    - Central Machine
        - CPU
        - Main memory
        - I/O Channels
        - System Operator's Console
        - Component boards
        - Keyboards
        - Monitors
        - Terminals
        - Cables
        - Connections
    - Workstations
    - Microcomputers
    - Storage medium
        - Magnetic Media
            - Disk pack
            - Magnetic tapes
            - Diskettes (floppies)
            - Cassettes
            - Drums
        - Nonmagnetic media
            - Punch cards
            - Paper tape
            - Paper printout
    - I/O Devices
        - User directed I/O devices
            - Printer
            - Card reader
            - Card punch
            - Paper tape reader
            - Terminals - local or remote
        - Storage I/O devices
            - Disk drives
            - Tape drives

- Communications equipment
  Communications lines
  Communications processors
  Controllers
  Multiplexers
  Switching devices
  Telephones
  Cables
  Modems
  Encryption Devices

- Special Interface Equipment
  Network front ends
  Intelligent controllers

2. Software
   - Operating System kernel

   - System Utilities

   - System Programs (compilers)

   - Programs
     Applications
     Standard application/operating programs
     Test programs
     Communications programs
     Source Programs
     Object Programs
     Maintenance diagnostic programs

3. Information (Data)
   - Data in execution

   - Data in Storage
     On magnetic medial
     Printed data
     Archival

   - Data in Transmission

   - Audit records

- Multilevel classification
    - Level I - Classified
        - Top Secret
        - Secret
        - Confidential
    - Level II - Sensitive Unclassified
        - Privacy Act data
        - Sensitive Business data
        - For official use only (FOUO)
            - Financial
            - Sensitive Management
            - Proprietary
            - Privileged
    - Level III - Unclassified
        - All other

4. Facilities
    - Environmental systems
        - Air-conditioning
        - Power
        - Water
        - Lighting
    - Building
    - Computer facility
        - Computer room
        - Data reception
        - Tape / disk library
        - Customer engineer room
        - I/O area
        - Data preparation area
        - Physical plant room
    - Backup equipment
        - Auxiliary power
        - Auxiliary environmental controls
        - Auxiliary supplies
    - Supplies
        - Magnetic media
        - Paper
        - Ribbons

5. Personnel/Human Resources

- Computer Personnel
  - Supervisory personnel
  - Systems analysts
  - Programmers
    - Applications programmers
    - Systems programmers
  - Operators
  - Librarian
  - Security officer
  - Maintenance personnel
  - Temporary employees
  - Consultants
  - System evaluators and auditors
  - Clerical personnel

- Building personnel
  - Janitors
  - Guards
  - Facility engineers
  - Installation management

6. Administrative/Operating Procedures

- Operations
  - Schedules
  - Operating guidelines and manuals
  - Audit documents

- Procedures
  - Emergency plans
    - Continuity of Operation Plans (COOP)
    - Disaster Recovery Plans
  - Security procedures
  - I/O procedures
  - Integrity controls

- Inventory records

- Operational procedures
  - Vital records
  - Priority run schedule
  - Production procedures

7. Documentation
- Software
- Hardware
- File
- Program
- JCL
- System

8. Supplies
- Magnetic media
- Paper
- Ribbons
- Forms
- Printer fluid

APPENDIX B (MAGNETIC MEDIA CONTROL)

Media marking

- Marked to accurately reflect the sensitivity of the information. Marking may be performed manually or automatically.

- Label storage media to reflect:
  - The sensitivity level of the information they contain.
  - Date of creation and destruction.
  - Unique identification number.
  - Creator or user.

- Color coding. Color coding of magnetic media or components shall comply with standard color codes for classified material.

Storage

- Media and containers. Media and containers should be marked/protected to the highest security classification level or most restrictive category of information stored on media **until** the media is declassified (degaussed/erased) or the information declassified/downgraded.

- Inventory Control.

- Access Control. Physical access to media in storage is often overlooked. A strong tendency is to protect the system while not providing equal measures for backup/stored data.

Destruction

- Destroy storage media in accordance with the organization's security provisions.

- Educate users to the proper methods for erasing or destroying storage media.

- Degaussing. Demagnetizing magnetic storage media (reduce magnetic flux to zero applying (coercive) magnetic force).

- Clearing vs. Declassification.
  - Clearing procedure. Accomplished by the overwrite of classified or sensitive material. Since the totality of declassification is lacking, cleared medial should not be released to subjects lacking access rights to the original material.

  - Declassification procedure. Accomplished by the obliteration of classified or sensitive material. Proper inventory control records will denote declassification events. The declassified media is releasable without restriction.

- Emergency destruction. Addressed as policy in risk management and contingency planning programs for the intentional mass destruction of media and other material which are classified or sensitive.

Media security

- Protect and secure information system storage media.

- Maintain, control, and audit storage media inventories.

- Password protection.

- Removable media.
  - Encourage use of removable, securable data storage systems.

  - Avoid fixed hard disks, especially if the system is used for classified applications.

- Control of printer ribbon. Control at the highest level of information printed. The ribbon should be retained in printer for life-cycle if physical controls permit.

Accountability

- Publicize procedures and policies to staff.

- Ensure that access for storing, transmitting, marking, handling, and destroying storage medial is granted only to authorized persons.

APPENDIX C (CONTINGENCY PLANNING AND BACKUP)

Contingency Plan Outline:

- Introduction
- Purpose
- Objectives
  - Considerations
  - Assumptions
  - Structure

- Preparations
  - Applications
  - Critical Processing Lists
  - Application Backup
  - Support agreement(s)

- Emergency Actions
  - Minimize the impact
    Protect life and property
    Minimize disruption to information system operation
  - Backup operations
  - Develop backup procedures
  - Maintain backup copies of application programs data files, and supporting documentation.

- Recovery operations
  - Develop plans to permit rapid restoration of information system facility operations

- Perform required periodic testing

- Contingency Plan testing
  - Not always time for response to read procedures
  - Most critical aspect of successful planning
  - Conduct frequent tests to maintain readiness
  - Minimally, plans will be tested once annually

LIST OF REFERENCES

Ahituv, N., and Sadan, B., "Learning to Live in a Distributed World," *Datamation*, v. 31, n. 18, pp. 139-148, September 1985.

Ahituv, N., and Neumann, S., *Principles of Information Systems For Management*, Third Edition, Wm. C. Brown Publishers, Dobuque, Iowa, 1990.

Bequai, A., *How to Prevent Computer Crime*, John Wiley & Sons, New York, NY, 1983.

Branstad, D.K., "Considerations for Security in the OSI Architecture," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987, pp. 9-14.

Browne, P.S., *Security: Checklist for Computer Center Self-Audits*, American Federation of Information Processing Societies, Arlington, VA, 1979.

Browne, P.S., "How to Manage the Network Security Problem," *Computer Security Journal*, v. 3, n. 1, pp. 77-87, Summer 1984.

Buchanan, J.R., and Linowes, R.G., "Understanding Distributed Data Processing," *Harvard Business Review*, pp. 143-153, July-August 1980.

Buchanan, J.R., and Linowes, R.G., "Making Distributed Data Processing Work," *Harvard Business Review*, pp. 143-161, September-October 1980.

Bynon, D.W., "Security Alert," *HP Professional*, v. 4, n. 7, pp. 26-30, July 1990.

Chalmers, L.S., "An Analysis of the Differences Between the Computer Security Practices in the Military and Private Sectors," *IEEE Symposium on Security and Privacy*, pp. 71-74, 1986.

Clark, D.D., and Wilson,D.R., "A Comparison of Commercial and Military Computer Security Policies," *IEEE Symposium on Security and Privacy*, pp. 184-194, 1987.

Commander, Naval Data Automation Command (COMNAVDAC), *The Department of the Navy (DON) Automated Information Systems (AIS) Security (DONAISS) Guidelines*, 1991.

International Business Machines Corporation (IBM), *Good Security Practices for Information Ownership and Classification*, 1986.

International Business Machines Corporation (IBM), *Guidelines for an Asset Protection Program in a Data Processing Environment*, 1986.

International Business Machines Corporation (IBM), *Good Security Practices for Information Systems Networks*, 1987.

Jackson, C.B., "The Need For Security," *Datapro Research*, v. 1, n. IS09-320-101, pp. 101-107, June 1990.

Jackson, C.B., "The Need For Security," *Datapro Research*, v. 1, n. IS09-100-101, pp. 101-134, October 1990.

Johnson, H.L., and Layne,J.D., "A Mission-Critical Approach to Network Security," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987, pp. 15-24.

King, P., "Disaster Planning," *HP Professional*, v. 4, n. 7, pp. 34-40, July 1990.

Lace, L., "Network Security," *DEC Professional*, v. 9, n. 9, pp. 38-47, September, 1990.

Lorin H., *Aspects Of Distributed Computer Systems*, Wiley-Interscience, New Work, NY, 1988.

McNurlin, B.C., and Sprague, R.H. Jr., *Information Systems Management In Practice*, Prentice Hall Press, Englewood Cliffs, NJ, 1989.

Menkus, B., "Understanding Data Communications Security Vulnerabilities," *Computers & Security*, v. 9, n. 3, pp. 209-213, May 1990.

Menkus, B., "Why Data Communications are Insecure," *Computers & Security*, v. 9, n. 6, pp. 483-487, October 1990.

Muftic, S., *Security Mechanisms For Computer Networks*, Ellis Horwood Limited, Chichester, England, 1989.

National Computer Security Center (NCSC), DOD 5200.28-STD, *Department of Defense Trusted Computer Systems Evaluation Criteria, "The Orange Book"*, December 1985.

National Computer Security Center (NCSC), CSC-STD-003-85, *Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, "The Yellow Book"*, 25 June 1985.

National Computer Security Center (NCSC), NCSC-TG-005-ver1, *Trusted Network Interpretation, "The Red Book"*, 31 July 1987.

National Computer Security Center (NCSC), NCSC-TG-011-ver1, *Trusted Network Interpretation Environments Guideline*, 1 August 1990.

National Institute of Standards (NIST), NIST Special Publication 500-600, *Computer Viruses and Related Threats: A Management Guide*, by J.P. Wack and L.J. Carnahan, 1987

Neugent, W., "Guidelines for Specifying Security Guards," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989, pp 320-338.

Palmer, I.C., and Potter, G.A., *Computer Security Risk Management*, Van Nostrand Reinhold, New York, NY, 1990.

Pfleeger, C.P., *Security In Computing*, Prentice Hall Press, Englewood Cliffs, NJ, 1989.

Phillips, R. Jr., "Computer Viruses: A Threat for the 1990s," *Datapro Research*, v. 1, n. IS09-250-101, pp. 101-121, October 1990.

Powell, D., "Network Abuse: Who's the Enemy?," *Networking Management*, v. 8, n. 9, pp. 27-34, September 1990.

Rutledge, L.S., and Hoffman, L.J., "A Survey of Issues in Computer Network Security," *Computers & Security*, v. 5, n. 4, pp. 269-308, December 1986.

Schaefer, M., "Network Security Assurance," *8th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 30 September - 3 October 1985, pp. 64-69.

Secretary of the Navy, SECNAVINST 5239.2 DONIRM, *Department of the Navy (DON) Automated Information Systems (AIS) Security Program*, 15 November 1989.

Stallings, W., "A Network Security Primer," *Computerworld*, v. XXIV, n. 5, pp.63-66 and 70, 29 January, 1990.

Stephenson, P., "Safe and Secure," *LAN Magazine*, v. 6, n. 9, pp. 34-44, September 1991.

Tate, P., "Risk! The Third Factor," *Datamation*, v. 34, n. 8, pp. 58-64, 15 April 1988.

Troy, E.F., "Dial-Up Security Update," *8th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 30 September - 3 October 1985, pp. 124-132.

Winters, P., "Secure Systems Design - An Evolving National Strategy," *Computers & Security*, v. 9, n. 5, pp. 379-389, August 1990.

Wood, C.C., "Fifteen Major Forces Driving the Civilian Information Security Market," *Computers & Security*, v. 9, n. 8, pp. 677-687, September 1990.

Wood, C.C., "Using information Security to Achieve Competitive Advantage," *Computers & Security*, v. 10, n. 5, pp. 399-404, August 1991.

BIBLIOGRAPHY

Abrams, M.D., "Observations on Local Area Network Security," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Abrams, M.D., and Podell, J.J., "Access Control and Authentication," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Abrams, M.D., and Podell, J.J., "Encryption," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Abrams, M.D., and Podell, J.J., "Network Security Overview," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Abrams, M.D., and Podell, J.J., "Protocols," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Abrams M.D., and Jeng, A.B., "Network Security: Protocol Reference Model and the Trusted Computer System Evaluation Criteria," *IEEE Network Magazine*, v. 1, n. 2, April 1987.

Allen-Tonar, L., "Networked Computers Attract Security Problems, Abuse," *Networking Management*, December 1989.

Anderson J., "A Unification of Computer and Network Security Concepts," *IEEE Symposium on Security & Privacy, IEEE Computer Society Press*, 1985.

Arbo, R.S., Johnson, E.M., and Sharp, R.L., "Extending Mandatory Access Controls to a Networked MLS Environment," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Arnold,T.S., "Multilevel Security From a Practical Point of View," *8th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 30 September - 3 October 1985.

Arsenault, A.W., "Developments in Guidance for Trusted Computer Networks," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

Axner, D., "Security Devices Prevent the Compromise of Network Resources," *Networking Management*, February 1990.

Baker, K.L., and Kirkpatrick, K. "The SILS Model for LAN Security," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Balenson, D.M., "Automated Distribution of Cryptographic Keys Using the Financial Institution Key Management System," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Berger J.L., Picciotto, J., Woodward, J.P.L., and Cummings, P.T., "Compartmented Mode Workstation: Prototype Highlights," *IEEE Transactions on Software Engineering*, v. 16, n. 6, June 1990.

Bologna, J., "Ethical Issues of the Information Era," *Computer & Security*, v. 9, n. 8, December 1990.

Brand, S., "A Status Report on the Development of Network Criteria," *8th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 30 September - 3 October 1985.

Branstad, M., Barker, W.C., Cochrane, P., and Balenson, D., "Key Management and Access Control for an Electronic Mail System," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Brown, D.C., and Teng, H.S., "An Expert System Approach to Security Inspection of a VAX/VMS System in a Network Environment," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

Burk, H., and Pfitzman, A., "Value Exchange Systems Enabling Security and Unobservability," *Computers & Security*, v. 9, n. 8, December 1990.

Bynon, David W., "A Plan for Avoiding Disaster," DEC Professional, v. 9, n. 9, September 1990.

Carrol, J.M., and Landweher, C.E., "Hardware Requirements for Secure Computer Systems: A Framework," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1984.

Clark, D.D., and Wilson, D.R., "Evolution of A Model for Computer Security," *11th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 17 - 20 October 1988.

Claybrook, B.G., "Using Views in a Multilevel Secure Database Management System," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1983.

Department of Defense Directive 5200.28, *Security Requirements for Automated Information Systems (AIS)*, 21 March 1988.

Department of Defense OPNAV Instruction 5239.1A CH-1, *Department of the Navy Automatic data Processing Security Program Instruction; revision to*, 1 April 1985.

Dion, L.C., "A Complete Protection Model," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1981.

Dobson, J.E., and Randell, B., "Building Reliable Secure Computing Systems Out of Unreliable Insecure Components," IEEE *Symposium on Security & Privacy, IEEE Computer Society*, 1986.

Estrin, D., and Tsudik, G., "Visa Scheme for Inter-Organization Network Security," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1987.

Fellows, J., Hemenway, J., Kelem, N., and Romero, S., "The Architecture of a Distributed Trusted Computing Base," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

Gasser, M., and Sidhu, D.P., "A Multilevel Secure Local Area Network," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1982.

Gasser, M., Goldstein, A., Kaufman, C., and Lampson, B., "The Digital Distributed System Security Architecture," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Glasgow, J.I., and MacEwen, G.H., "A Two-Level Security for a Secure Network," *8th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 30 September - 3 October 1985.

Government Services Administration, FIRMR Bulletin 30, *Use of Small Government Owned Computers off Site and Use of Personally Owned Computers in Federal Offices*, 15 October 1985

Graft, D., Pabrai, M., and Pabrai, U., "Methodology for Network Security Design," *IEEE Communications Magazine*, November 1990.

Greenlee, Fr. M.B., "Requirements for Key Management in the Wholesale Fin ncial Services Industry," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Hartman, B., and Taylor, T., "Formal Models, Bell and LaPadual, and Gypsy," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

Juitt, D. "Security Assurance Through System Management," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Jueneman, R.R., "Electronic Document Authentication," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Kak ,S.C., "Data Security in Computer Networks," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Keith, E.L., "Space Shuttle Security Policies and Programs," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Kent, S.T., and Voydock, V.L., "Security in High-Level Network Protocols," *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Kerut, E.G., and Tater, G.L., "The Secure Data Network System: An Overview," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

Korelsky, T., and Sutherland, D., "Formal Specification of a Multi-Level Secure Operating System," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1984.

Kruys, J.J., "Progress in Secure Distributed Systems," *Computers & Security*, v. 10, n. 5, pp. 429-441, August 1991.

Lathrop, D., "Perestroika and its Implications for Computer Security in the U.S.S.R.," *Computers & Security*, v. 9, n. 8, December 1990.

Loscocco, P., "A Security Model and Policy for a MLS LAN," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

Lu Wen-Pai and Sundareshan M.K., "A Model for Multilevel Security in Computer Networks," *IEEE Transactions on Software Engineering*, v. 16, n. 6, June 1990.

Lubarsky, R.S. "Evaluation of Security Model Rule Bases," 12th *National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Lusa, J.M., "Editor's Notes, The First Rule of Network Security: Have a Policy," *Networking Management*, September 1990.

McGill Lu, M., and Mayer, B.A., "Guidelines for Formal Verification Systems: Overview and Rational," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

McLean, J., "Reasoning About Security Models," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1987.

Nelson, R., "SDNS Services and Architecture," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

Nessett, D.M., "Factors Affecting Distributed System Security," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1986.

Norvell, W. "Integration of Security into the Acquisition Life Cycle," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

O'Dell, L.L., "An Approach to Multi-Level Secure Networks Revision 1," *8th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 30 September - 3 October 1985.

Page, J., Heaney, J., Adkins, M., and Dolsen, G., "Evaluation of Security Model Rule Bases," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Parker, T.A., "Application Access Control Standards for Distributed Systems," *Computers & Security*, v. 9, n. 6, October 1990.

Powell, D., "Fighting Network Infection," *Networking Management*, September 1989.

Public Law 100-235, *Computer Security Act of 1987*, 8 January 1988.

Research Institute for Advanced Computer Science, NASA Ames Research Center, *Access Control and Privacy in Large Distributed Systems*, B.M. Leiner, and M. Bishop, 7 March 1986.

Rushby, J., "Networks are Systems", *Tutorial Computer and Network Security/Proceedings, IEEE Computer Society Press*, 1987.

Ruthberg, Z.G., "Guide to Auditing for Controls and Security: A System Life Cycle Approach," *11th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 17 - 20 October 1988.

Saydjari, O.S., Beckman, J.M., and Leaman, J.R.,"Locking Computers Securely," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

Saydjari, O.S., Beckman, J.M., and Leahman, J.R., "LOCK Trek: Navigating Uncharted Space." *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1989.

Schaefer, M., "Symbol Security Condition Considered Harmful," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1989.

Schell, R.R., Colonel, USAF, "Evaluating Security Properties of Computer Systems," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1983.

Schnackenberg, D.D., "Development of a Multilevel Secure Local Area Network," *8th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 30 September - 3 October 1985.

Schnackenberg, D.D., "Applying the Orange Book to an MLS LAN," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

SECNAVINST 5239.2 DONIRM, *Department of the Navy (DON) Automated Information Systems (AIS) Security Program*, 15 November 1989.

Sheehan, E.R., "Access Control Within SDNS," *10th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 21 - 24 September 1987.

Smid, M., Dray, J. and Warnar, R.B.J., "A Token Based Access Control System for Computer Networks," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Stevens, J.A., and Weiner, R.E., "A Structured Approach to Risk Assessment: An Innovative Concept," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Stoneburner, G.R., and Snow, D.A., "The Boeing MLS LAN: Headed Towards an INFOSEC Security Solution," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Tasker, P.S., "Trusted Computer Systems," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1981.

Taylor, T., "Comparison Paper Between the Bell and LaPadula Model and the SRI Model," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1984.

U.S. Department of Commerce, National Bureau of Standards, NBS Special Publication 500-21, Volume 1, *Design Alternatives for Computer Network Security*, G.D. Cole, edited by D.K. Branstad, January 1978.

U.S. Department of Commerce, National Bureau of Standards, NBS Special Publication 500-21, Volume 2, *The Network Security Center: A System Level Approach to Computer Network Security*, F. Heinrich, January 1978.

Varadharajan, V., and Black, S., "Formal Specification of a Secure Distributed Messaging System," *12th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 10 - 13 October 1989.

Varadharajan, V., "Verification of Network Security Protocols," *Computers & Security*, v. 8, n. 8, December 1990.

Varadharajan, V., and Black, S., "Multilevel Security in a Distributed Object-Oriented System," *Computers & Security*, v. 10, n. 1, February 1991.

Vickers Benzel, T.C., "Trusted Software Verification: A Case Study," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1985.

Walker, S., "Network Security Overview," *IEEE Symposium Security & Privacy, IEEE Computer Society*, 1985.

Walker, S., "The Computer Security Act of 1987, A Focus on How NIST/NSA Will Interact on Policy, Implementation, and Technology," *11th National Computer Security Conference Proceedings, National Bureau of Standards/National Computer Security Center*, 17 - 20 October 1988.

Walker, S., "Network Security: The Parts of the Sum," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1989.

Weiss, J., "Five Ways to Secure Your Network," *TPT Magazine*, September 1988.

Withington, P.T., "The Trusted Function in Secure Decentralized Processing," *IEEE Data Security & Privacy, IEEE Computer Society*, 1980.

Wood, C.C., "Principles if Secure Information Design," *Computers & Security*, v. 9, n. 1, February 1990.

Woodie, P.E., "Security Enhancement Through Product Evaluation," *IEEE Symposium on Security & Privacy, IEEE Computer Society*, 1983.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
Cameron Station
Alexandria, Virginia 22304-6145

2. Library, Code 52 2
Naval Postgraduate School
Monterey, California 93943-5002

3. Professor Myung Suh 1
Department of Administrative Sciences
Code AS/Su
Naval Postgraduate School
Monterey, California 93943

4. Professor Moshe Zviran 1
Department of Administrative Sciences
Code AS/Zv
Naval Postgraduate School
Monterey, California 93943

5. Lieutenant Donovan R. Rhead 1
8632 Braile
Detroit, Michigan 48228